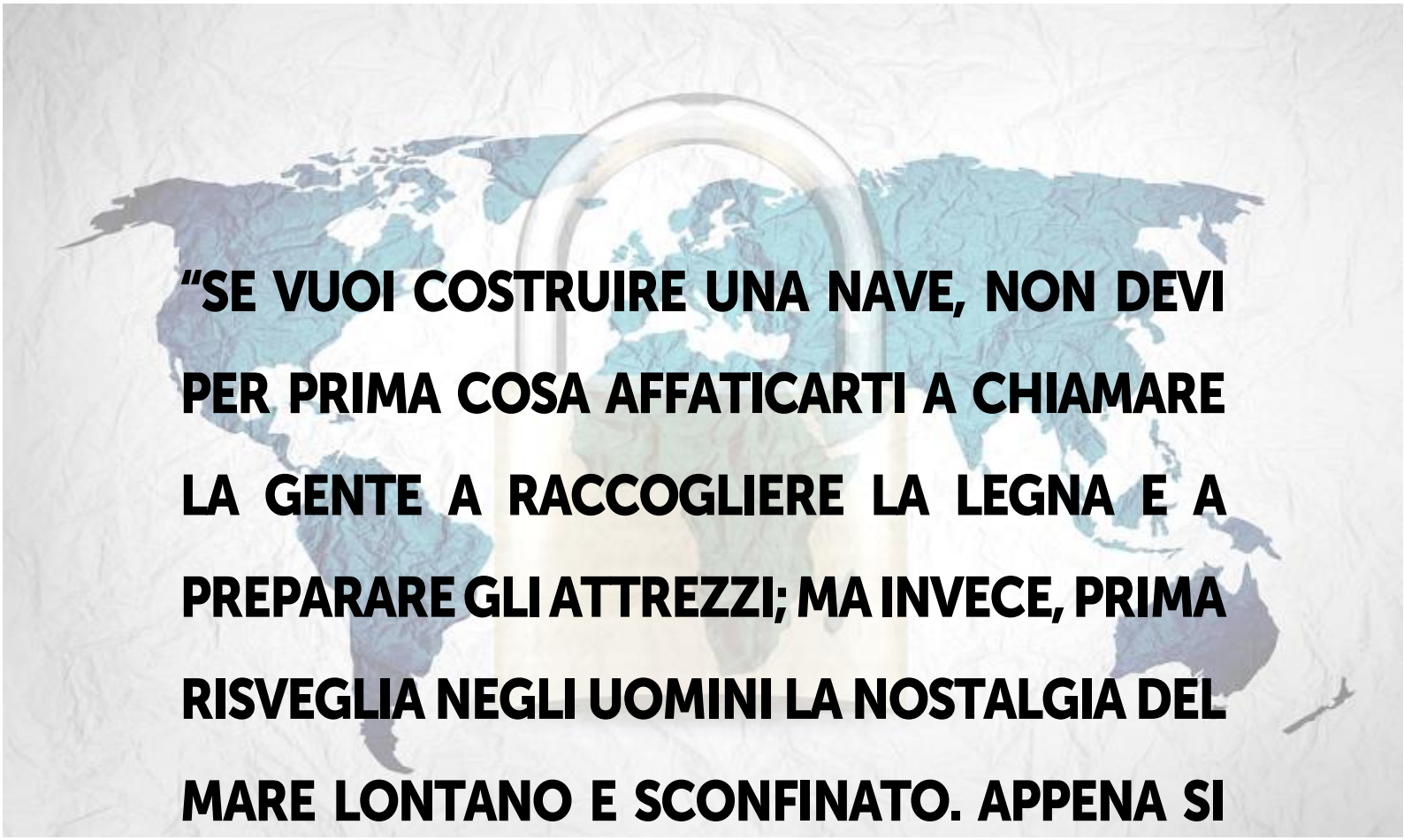
COME GESTIRE LA PRIVACY

REG. (UE) 2016/679

VADEMECUM PER MAESTRI DI SCI E SCUOLE DI SCI

In collaborazione con

Qualità . Sicurezza . Ambiente



"SE VUOI COSTRUIRE UNA NAVE, NON DEVI PER PRIMA COSA AFFATICARTI A CHIAMARE LA GENTE A RACCOGLIERE LA LEGNA E A PREPARARE GLI ATTREZZI; MA INVECE, PRIMA RISVEGLIA NEGLI UOMINI LA NOSTALGIA DEL MARE LONTANO E SCONFINATO. APPENA SI SARÀ RISVEGLIATA IN LORO QUESTA SETE SI METTERANNO SUBITO AL LAVORO PER COSTRUIRE LA NAVE."

ANTOINE DE SAINT EXUPÈRY

INDICE

1 INTRODUZIONE

È sempre più evidente la profonda riforma che sta interessando la protezione dei dati personali in ambito europeo, aspetto che, da qualche mese, si pone come costante nella nostra quotidianità.

Questo perché, a partire dal 25 maggio 2018, è stata data piena attuazione al Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati (in seguito, GDPR, ovvero *General Data Protection Regulation*).

La nuova normativa comunitaria ha profondamente innovato l'approccio precedente, ponendo con forza l'accento sulla responsabilizzazione (*accountability* nell'accezione inglese) di Titolari e Responsabili del trattamento – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare un'efficace e sostanziale tutela dei dati personali, nonché l'applicazione del regolamento. Si tratta di una grande novità, in quanto viene affidato ai Titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative vigenti. La protezione dei dati personali, alla luce della nuova normativa europea, non si risolve nel mero assolvimento di singoli adempimenti formali, ma richiede la costruzione di una struttura organizzativa preposta a tal scopo.

Il Regolamento si pone, quindi, come guida e stimolo alla creazione di un sistema di *data protection* specifico per ogni realtà (dalla grande società, alla PMI), in cui si tenga conto delle peculiarità di ogni contesto e degli elementi che caratterizzano il trattamento dei dati, giacché solo dal basso è possibile contribuire allo sviluppo di un idoneo sistema di protezione, che sia davvero corrispondente alle finalità di tutela che l'impianto normativo vuole suggerire.

Il presente Vademecum è volto ad accompagnare l'utente (Scuola di Sci o singolo Maestro, in seguito anche, più generalmente, "Associato") nell'applicazione del GDPR. Il documento, comprensivo degli strumenti operativi che lo compongono, ha però carattere generale e pertanto, va adattato da ogni lettore alla propria realtà.

Ogni Associato, quando usa dati personali, dovrà quindi adempiere a quanto previsto dal Regolamento, con un'azione dedicata agli ambiti di operatività interessati dalla normativa *privacy*.

Scopo del presente Vademecum, specifico per la nostra categoria, è quello di indicare e consigliare un *modus operandi* che rispetti le misure minime standard che le Scuole di sci ed i Maestri di sci devono adottare per poter adempiere alla normativa citata.

1.1 GUIDA ALLA LETTURA

Il presente Vademecum è stato strutturato per consentire al lettore una lettura su più livelli.

La **prima parte** del documento illustra ed analizza l'impianto normativo vigente in materia di protezione dei dati personali. Pertanto, i paragrafi dedicati forniscono al lettore le definizioni necessarie alla conoscenza della norma e alla conduzione di un'attività di adeguamento consapevole.

Nella **seconda parte** intitolata "*Come adeguarsi al GDPR ed al D.LGS. 101/18*" (pag. 20), si procede all'approfondimento dei singoli adempimenti prescritti per realizzare la piena conformità normativa, seguito dall'applicazione guidata degli stessi alla realtà esaminata.

Con gli **STRUMENTI OPERATIVI**, infine, vengono forniti dei modelli generali della documentazione formale prescritta per la protezione dei dati personali (pag. 48).

Si ricorda che la modulistica ha carattere generico e deve pertanto essere adattata alle specificità di ogni Scuola di sci o libero professionista, a seguito di una mirata analisi dei trattamenti operati.

2 NORMATIVA

In quanto Regolamento europeo, il GDPR è un atto a portata generale, obbligatorio in tutti i suoi elementi, e direttamente applicabile in ciascun Stato membro. Ciò significa che le norme interne restano in vigore solo in quanto compatibili con il nuovo impianto normativo comunitario. Il legislatore italiano, sul punto, ha recentemente provveduto ad emanare un decreto di armonizzazione, sulla base della Legge di delegazione europea 2017, al fine di adeguare la normativa nazionale vigente (ovvero il Codice in materia di protezione dei dati personali, d.lgs. 196/2003) alle disposizioni del GDPR. Invero, il d.lgs. 101/2018, pubblicato nella Gazzetta Ufficiale della Repubblica Italiana in data 4 settembre 2018, ha novellato il Codice Privacy italiano, limitatamente agli aspetti che si ponevano in contrasto con il Regolamento UE, contribuendo così alla predisposizione di una disciplina normativa unitaria.

Nel prosieguo del documento, quindi, verranno considerate sia la normativa italiana, che quella europea, in un quadro normativo completo ed attuale, il quale tuttavia è rapportato allo stato dell'arte, e passibile di modifiche in conseguenza dell'evoluzione normativa e giurisprudenziale.

Inoltre, si consideri che, a livello internazionale, il diritto alla tutela dei dati personali assume rilievo anche in quanto contemplato dalla Convenzione europea dei diritti dell'uomo (CEDU), il cui art. 8 prevede il "*rispetto della vita privata e familiare*" e individua così il diritto alla protezione dei dati come diritto assoluto e fondamentale della persona, nonché dalla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (n. 108/1981), alla quale aderiscono 51 paesi, anche extra – europei. Ancora, con la Carta dei diritti fondamentali dell'Unione Europea, divenuta giuridicamente vincolante con l'entrata in vigore del Trattato di Lisbona nel 2009, la volontà è stata quella di assegnare alla protezione dei dati un valore ed una tutela autonoma rispetto agli altri diritti fondamentali (come il rispetto della vita privata e familiare, e il diritto alla libertà ed alla sicurezza).

3 SCUOLE DI SCI E MAESTRI DI SCI VS. PRIVACY

Il trattamento dei dati personali rappresenta un passaggio obbligato per ogni attività d'impresa, ed anche nel caso in cui l'attività sia svolta da parte del singolo Maestro associato. L'insegnamento della pratica sportiva, infatti, non può prescindere dalla conoscenza e dall'impiego di dati personali, in quanto necessari alla realizzazione di molteplici servizi offerti.

A tal fine, è importante, all'interno di ogni singola realtà interessata, individuare le tipiche attività quotidiane che prevedono operazioni di trattamento. Successivamente, si renderà indispensabile ricostruire il percorso effettuato da ciascun dato personale all'interno di ogni specifico trattamento, così da registrarne le caratteristiche rilevanti ai fini della tutela, e contestualmente determinarne i diversi flussi.

Sinteticamente, la normale attività svolta dalla Scuola di Sci, nonché dal singolo Maestro, interessa principalmente i dati dei clienti, sia minorenni che maggiorenni. La Scuola di Sci, inoltre, come realtà organizzata, effettua trattamenti anche su dati dei dipendenti, dei Maestri di sci associati, dei collaboratori esterni e dei fornitori. È possibile, infine, un'esternalizzazione di dati a soggetti terzi che eseguono servizi a favore del Titolare. Ogni processo appena elencato comporta l'adozione di particolari cautele in capo al Titolare del Trattamento (ovvero, alla Scuola o al Maestro).

Nel dettaglio, cerchiamo di esaminare quali sono i maggiori processi che comportano il trattamento di dati da parte degli associati AMSI, e che assumono particolare rilevanza in termini di protezione dei dati personali, fissandone gli adempimenti più significativi:

- **GESTIONE DEI RAPPORTI CON I CLIENTI:** La Scuola di Sci, nonché il singolo Maestro di Sci che lavora in autonomia, trattano quotidianamente i dati personali dei clienti (maggiorenni e minorenni) che vogliono usufruire delle lezioni di sci e dei vari servizi offerti, dal momento del contatto diretto con l'utente, sino al pagamento della prestazione, diventando così Titolari dei dai raccolti.

  In particolare, la Scuola o il professionista gestiscono la prenotazione delle lezioni e dei corsi, e a tal fine si occupano di tutti gli aspetti fiscali e contrattuali nel rapporto con il cliente. Oltre a ciò, un trattamento rilevante ai fini dell'applicazione del Regolamento è la produzione (anche affidata a terzi), la raccolta e la diffusione di materiale fotografico, nonché la produzione di video interessanti il cliente, a scopo didattico/promozionale.

  Sempre in relazione al trattamento dei dati in formato multimediale, può capitare che i maestri di sci, nel corso della propria attività, facciano autonomamente fotografie o video, e le utilizzino sui propri social (aspetto, questo, molto delicato: cfr. pag. 30).

  In ultimo, per finalità pratiche di riconoscimento e/o di sicurezza, in occasione dei corsi dedicati ai bambini, le Scuole di Sci ed i Maestri sono soliti identificare i singoli partecipanti attraverso l'utilizzo di

una pettorina riportante nome e cognome del minore, oppure numero di telefono del genitore di riferimento abbinato al nome dell'allievo. Si dà atto che possono essere offerti anche servizi ulteriori, come ad esempio il servizio di asilo per bambini e le escursioni organizzate. Anche laddove la gestione degli stessi appartenga ad una società commerciale esterna, è probabile che la Scuola di Sci venga a contatto con i dati dei partecipanti. In questo caso, dovrà essere fornita un'informativa differenziata.
Di ogni trattamento dev'essere data informazione all'interessato: a tal fine viene utilizzato il principale strumento dell'informativa, la quale ovviamente dovrà differenziarsi a seconda dei servizi offerti, ed inoltre prevedere il consenso quando necessario per la legittimità del trattamento.

- **DATI DEI DIPENDENTI, DEI MAESTRI ASSOCIATI, DEI COLLABORATORI**: Per quanto attiene alla Scuola di Sci, si consideri che la stessa effettua trattamenti anche di dati dei dipendenti (ad esempio, del personale di segreteria, o dei maestri assunti o associati), nonché dei maestri operanti in regime di P.IVA. A tal fine, la Scuola raccoglie dati anagrafici, dati di contatto e bancari, numero della licenza ed attestazione dell'iscrizione all'albo. Tali dati non vengono diffusi, salvo per quanto riguarda eventuali fotografie e immagini video.
  A livello interno, è certamente importante informare l'interessato circa i trattamenti effettuati sui dati da parte della Scuola di Sci, ma appare fondamentale soprattutto effettuare la nomina ad Autorizzato al Trattamento dei dati, se il servizio affidato allo specifico dipendente, maestro assunto, associato, o collaboratore comporta il trattamento di dati personali.

- **DATI DEI FORNITORI**: Per quanto riguarda la comunicazione dei dati ad eventuali fornitori di servizi esterni, vi può essere esternalizzazione dei dati dei clienti, dei dipendenti e dei collaboratori, ad esempio, a commercialista, consulente del lavoro, assicurazione, servizio legale, fotografo, videomaker, tecnico informatico, tecnico che gestisce il sito web e l'area social media.
  In questo caso, è necessario elaborare una nomina a Responsabile esterno, che funge da vero e proprio contratto (accordo tra le parti) in ordine al trattamento di dati personali effettuato dal soggetto terzo per conto della Scuola di Sci.

Per un approfondimento in merito agli adempimenti riferiti ai singoli trattamenti, si rinvia al capitolo 8, paragrafo 8.1, a pag. 29.

4 DEFINIZIONI UTILI

4.1 Ambito oggettivo di applicazione

Di seguito vengono riportate alcune spiegazioni utili a comprendere meglio l'ambito di applicazione del Regolamento UE sulla protezione dei dati personali, discendenti principalmente dall'art. 4 del GDPR.

4.1.1 DATO PERSONALE:

Qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato). Tale generica formulazione consente di adattare la definizione di dato personale alla rapida evoluzione del progresso tecnologico. Si tratta di informazioni che riguardano una persona individuata (perciò distinguibile), o che può essere identificata mediante l'ausilio di informazioni aggiuntive. Pertanto, anche il solo nome e cognome, o il numero di cellulare di un soggetto, è un dato personale rilevante per il Regolamento, e come tale da tutelare;

4.1.2 TRATTAMENTO:

Per trattamento di dati personali si intende qualsiasi operazione che abbia ad oggetto o implichi l'impiego di dati personali.

Tra le tantissime attività individuate dall'art. 4 GDPR, che costituisce un elenco non esaustivo, basti sottolineare che anche la mera conservazione configura un trattamento di dati da eseguire con le dovute cautele;

4.1.3 PROFILAZIONE:

Si tratta dell'elaborazione dei dati relativi a uno o più clienti o utenti, allo scopo di suddividerli in gruppi omogenei in base a gusti, interessi e comportamenti. Se si effettua una simile attività, è fondamentale informare gli interessati dell'esistenza di una decisione basata sul trattamento di dati automatizzato comprendente profilazione, e prevedere la possibilità, per l'interessato, di esprimere il proprio consenso (o di rifiutare il trattamento automatizzato dei dati);

4.1.4 PSEUDONIMIZZAZIONE:

È una misura di sicurezza che prevede il trattamento di dati personali in modo da renderli non più riconducibili ad uno specifico soggetto interessato, senza utilizzo di informazioni aggiuntive (ad esempio, mediante la sostituzione del nominativo completo con le sole iniziali). Si precisa che, siccome il dato potrebbe essere riconducibile ad una persona fisica mediante ulteriori informazioni, si tratta comunque di informazione riguardante una persona fisica *identificabile*, ovvero di dato

personale. Il vantaggio, in questa tecnica (utilizzata soprattutto nel contesto della ricerca e della statistica), risiede nell'aumento di protezione del dato personale mediante un processo volto a mascherare l'identità. L'idea di base è che alcune informazioni siano visibili, ma risultino allo stesso modo incomprensibili, in quanto separate dagli elementi necessari a dar loro un senso. È per questo motivo che la pseudonimizzazione si distingue dal concetto di anonimizzazione, che prevede una de - identificazione irreversibile tale da non consentire più di risalire al dato dettagliato;

4.1.5 PARTICOLARI CATEGORIE DI DATI (art. 9 GDPR):

Ci si riferisce a dati che rivelano *l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale di una persona*. Sono i dati che, nell'accezione ante – GDPR, erano chiamati "dati sensibili". Il Regolamento impone un divieto generale di trattamento di tali dati, salvo per alcune condizioni legittimanti indicate nel comma 2 dell'art. 9 (prima fra tutte, il consenso dell'Interessato). Dai dati comuni si distinguono anche i dati relativi a condanne penali e reati: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. L'art. 10 GDPR prevede che il trattamento dei dati personali relativi a condanne penali e reati deve avvenire sotto il controllo dell'Autorità Pubblica, ovvero a seguito di autorizzazione proveniente dal diritto dell'Unione o degli Stati, che preveda garanzie appropriate per i diritti e le libertà dei cittadini. Nel dettaglio, l'art. 2 – *octies* co. 3 del d.lgs. 196/2003, come modificato dal d.lgs. 101/2018, specifica le ipotesi di autorizzazione prevista da norme di legge o, nei casi previsti dalla legge, di regolamento (ad esempio, adempimento di obblighi ed esercizio di diritti da parte del Titolare o dell'Interessato in materia di diritto del lavoro, l'accertamento di responsabilità in relazione a sinistri, infortuni, o eventi attinenti alla vita umana – per il corretto esercizio dell'attività assicurativa – e l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria).

Tali dati particolari necessitano di più cautele nel loro trattamento, giacché si riferiscono ad informazioni cd. personalissime e delicate;

4.1.6 DATI COMUNI:

Tutti i dati personali che NON rientrano nell'elencazione sopra riportata e relativa a "particolari categorie di dati". Si suddividono in dati che permettono l'identificazione diretta, come quelli anagrafici, di contatto o bancari, e dati che permettono l'identificazione indiretta, come ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa. Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti (con riferimento al controllo sui lavoratori, effettuato per mezzo di tali strumenti, si veda pag. 33).

4.2 Ambito soggettivo di applicazione

Il Regolamento individua nuovi soggetti che interessano la protezione dei dati personali, ed ha provveduto a modificare l'assetto delle responsabilità. Ecco i protagonisti in materia di *privacy*:

4.2.1 TITOLARE DEL TRATTAMENTO:

È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Si tratta, sostanzialmente, del soggetto che determina autonomamente "perché" e "come" devono essere trattati i dati personali.

Con riferimento al caso di specie, sono Titolari del Trattamento le Scuole di Sci ed i Maestri di Sci che lavorano in forma autonoma.

Il Titolare, in quanto tale, esercita una vera e propria Titolarità sui dati, ed è giuridicamente responsabile per qualsiasi trattamento eseguito direttamente o effettuato da terzi per suo conto (salvo che non intervenga una nomina a Responsabile esterno ai sensi dell'art. 28 GDPR, come spiegato nel paragrafo successivo).

L'art. 24 GDPR gli impone di mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, suscettibili di cagionare un danno fisico, materiale o immateriale.

A fronte di un danno derivante dalla violazione delle norme vigenti in materia di protezione dei dati personali, il Titolare ne risponde direttamente.

4.2.2 RESPONSABILE DEL TRATTAMENTO:

È *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo* (distinto dal Titolare) *che tratta dati personali per conto del Titolare del Trattamento*.

In concreto, ai sensi dell'art. 28 GDPR; la figura del "Responsabile del trattamento" coincide con i soggetti che svolgono servizi a favore del Titolare implicanti il trattamento di dati su cui il Titolare esercita il proprio potere / controllo. Parliamo quindi di terzi fornitori che, a qualunque titolo, intervengono nel trattamento dei dati facenti capo al Titolare, svolgendo per quest'ultimo un'attività di elaborazione dei dati, indispensabile per l'esecuzione del servizio affidatigli ed il raggiungimento delle finalità del trattamento dallo stesso stabilite (a titolo esemplificativo e non esaustivo, commercialista, consulente del lavoro, assicurazione, servizio legale, fotografo, videomaker, tecnico informatico, tecnico o soggetto che gestisce il sito web e l'area social media). Al pari di ogni altro soggetto che agisca sotto l'autorità del Titolare del trattamento, il Responsabile deve essere autorizzato ed istruito chiaramente sulle modalità e i limiti del trattamento.

In tal senso, il GDPR, all'art. 28, stabilisce che i trattamenti eseguiti dal responsabile debbano essere disciplinati da un contratto o altro atto giuridico che vincoli il responsabile del trattamento al Titolare del trattamento e che regoli la materia disciplinata, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti delle parti.

Col contratto, conformemente a quanto stabilito dell'art. 28 del nuovo Regolamento, il Titolare, di fatto, delega al responsabile la concreta gestione del trattamento, affidandogli uno o più compiti specifici, oppure una serie di compiti dettagliati.

Nel caso in cui il responsabile del trattamento ecceda i limiti di utilizzo dei dati fissati dal titolare, diventa titolare della gestione illecita degli stessi e ne risponde come tale. Appare importante, quindi, definire con chiarezza i trattamenti affidati al Responsabile esterno, per limitare la propria responsabilità nel caso vi dovessero essere violazioni riconducibili al solo operato del Responsabile. Affinché operi tale condizione esimente, è però necessario che il Titolare del trattamento abbia scelto e designato il Responsabile del trattamento dopo un'attenta valutazione circa l'affidabilità dello stesso. Infatti, ai sensi della normativa europea è prescritto che il Titolare possa ricorrere unicamente a Responsabili che prestino sufficienti garanzie circa la capacità di tutelare in modo adeguato i dati consegnatigli.

Per una tutela sostanziale, il Responsabile è soggetto a veri e propri obblighi sanciti dal Regolamento, che possono così riassumersi:

- obbligo di trasparenza. Il Responsabile del trattamento deve mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del Regolamento, e dovrà tenere il registro dei trattamenti svolti (ex art. 30, paragrafo 2, GDPR);
- obbligo di garantire la sicurezza dei dati. Così come il Titolare, anche il Responsabile deve adottare tutte le misure di sicurezza adeguate al rischio (art. 32 GDPR), tra le quali anche le misure di attuazione dei principi di *privacy by design* e *by default*. Deve, inoltre, garantire la riservatezza dei dati, vincolando i dipendenti, ed occuparsi della cancellazione dei dati alla fine del trattamento. Infine, deve informare il Titolare delle eventuali violazioni avvenute;
- obbligo di avvisare, assistere e consigliare il Titolare. Il Responsabile deve consentire e contribuire alle attività di revisione, ed assistere il Titolare nel garantire il rispetto degli obblighi previsti dal Regolamento, per la parte di competenza.

Una precisazione: è possibile che il Responsabile del Trattamento, ricorra, a sua volta, ad un sub – responsabile, allorquando esternalizza parte del servizio di cui è incaricato ad un terzo. Questa operazione deve essere autorizzata in modo scritto dal Titolare, giacché il sub – responsabile sarà soggetto ad obblighi specifici per garantire la protezione del dato personale trattato. Si tratta, in sostanza, di una struttura a catena, ove i vari soggetti ai quali vengono esternalizzati dei servizi che implicano il trattamento di dati del Titolare vengono appositamente istruiti in tal senso dal Titolare stesso, contribuendo così alla creazione di un valido sistema integrato di *data protection*.

4.2.3 INTERESSATO:

È la persona fisica a cui si riferiscono i dati personali (ad esempio, il cliente che partecipa ai corsi di sci, sia esso maggiorenne che minorenne, il dipendente, il collaboratore). I dati delle persone giuridiche, invece, non sono oggetto di alcun obbligo di tutela, salvo il caso in cui tali dati si inseriscano in un servizio di comunicazione elettronica (provv. 262/2012, Autorità Garante della protezione dei dati personali), ed anche nell'ipotesi in cui da tali dati sia possibile desumere l'identità personale del soggetto Titolare.

Molti sono i diritti di che gli artt. 15 e seguenti del GDPR riconoscono all'Interessato, e che devono essere garantiti dai soggetti che eseguono un trattamento rilevante su quei dati personali: diritto di accesso, rettifica, integrazione e cancellazione dei dati, portabilità, limitazione del trattamento e revoca del consenso prestato; diritto di opporsi al trattamento o limitare l'accesso agli atti (salvo il caso in cui l'accesso sia necessario per esercitare e difendere un proprio diritto in giudizio), diritto di proporre reclamo all'Autorità di Controllo laddove l'Interessato ritenga che i Suoi dati

siano trattati in modo illegittimo e contrariamente alle prescrizioni legislative in materia, diritto ad essere informato in caso di violazione, nonché diritto al pieno ed effettivo risarcimento del danno, come previsto dall'art. 82 GDPR.

Si consideri che l'art. 23 GDPR prevede la possibilità per gli Stati membri di limitare la portata dei diritti appena elencati. Invero, l'art. 2 – *undecies* del d.lgs. 196/2003, così come modificato dal recentissimo d.lgs. 101/2018, sancisce alcune limitazioni specifiche e settoriali all'esercizio dei diritti da parte dell'Interessato, con richiesta al Titolare del trattamento ovvero con richiamo all'Autorità di controllo (Garante per la protezione dei dati personali), ad esempio in materia di riciclaggio o in caso di tutela della riservatezza dell'identità del dipendente che effettua segnalazioni di reati o irregolarità di cui sia venuto a conoscenza nell'ambito di un rapporto di lavoro).

4.2.4 DPO (Data Protection Officer)

È detto anche Responsabile per la Protezione dei Dati (RPD), ed è una figura introdotta dal nuovo Regolamento UE.

In pratica, il DPO è un consulente esperto che va ad affiancare il Titolare nella gestione delle problematiche inerenti al trattamento dei dati personali, con un ruolo misto di consulenza e controllo. Si tratta di un soggetto chiave, deputato a favorire l'osservanza della normativa in materia di protezione dei dati, seguendo non solo le disposizioni contenute nel Regolamento, ma anche considerando il panorama legislativo nazionale.

L'art. 37 GDPR elenca i casi in cui è obbligatoria la nomina di tale soggetto:

- Se il trattamento è effettuato da un'autorità pubblica o da un organismo di diritto pubblico, ad esclusione delle autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- Se le attività di *core business* (ovvero, l'attività principale) del Titolare o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- Se le attività di *core business* del Titolare o del Responsabile del trattamento consistono nel trattamento su larga scala di particolari categorie di dati (art. 9 GDPR) o di dati relativi a condanne penali e a reati (art. 10 GDPR).

NON essendo, questi, casi che interessano la realtà propria dell'Associato, è esclusa l'obbligatorietà della nomina di un DPO.

4.2.5 AUTORIZZATO AL TRATTAMENTO

La figura dell'Autorizzato del trattamento, fa riferimento ai dipendenti ed ai collaboratori che, nel Codice della *privacy* nazionale ante – riforma, venivano qualificati come "Incaricati del trattamento".

La figura degli Incaricati al trattamento, infatti, non è espressamente prevista dalla nuova disciplina europea in materia di protezione dei dati personali, ma se ne ricava la necessità dalla lettura complessiva dell'impianto normativo, il quale non ne esclude la nomina, facendo riferimento a persone autorizzate al trattamento dei dati che agiscono sotto l'autorità diretta del Titolare o del responsabile (cd. Autorizzati al Trattamento ai sensi dell'art. 4, GDPR). Si tratta, in sostanza, dei soggetti interni alla realtà organizzativa che effettuano trattamenti di dati per conto del Titolare (un esempio inerente alla realtà della Scuola di Sci: l'addetto alla segreteria che raccoglie i dati dei clienti che desiderano partecipare al corso di sci, oppure l'addetto alla contabilità che si occupa di emettere le fatture o riscuotere i pagamenti). Tali soggetti devono essere destinatari di una formale nomina ad "Autorizzato al trattamento".

É fondamentale fornire agli Autorizzati precise istruzioni operative, soprattutto in termini di obblighi di riservatezza e misure di sicurezza da rispettare nello svolgimento delle operazioni di trattamento accordate (art. 29 GDPR), e contestualmente assicurare loro la necessaria formazione. In caso contrario, infatti, anche in presenza di formali designazioni, queste sarebbero del tutto prive di valore.

4.2.6 MINORENNI

La questione relativa al trattamento di dati personali di soggetti minorenni merita un approfondimento specifico, giacché la minore età è legata a diritti rafforzati rispetto agli adulti, per cui il trattamento da parte delle aziende dei loro dati deve essere regolamentato in maniera differente. L'art. 8 GDPR (ed anche l'art. 2 – *quinques* del d.lgs. 196/2003, come aggiornato dal d.lgs. 101/2018) non riguarda genericamente tutti i trattamenti di dati di minori, ma solo il caso in cui vi sia un'offerta diretta di servizi della società dell'informazione a soggetti minori di 16 anni (per l'Italia si parla di 14 anni), e quindi riguarda principalmente il rapporto del minore con la rete e i suoi servizi. In tal caso, il trattamento è lecito solo se è basato sul consenso di colui che esercita la Responsabilità genitoriale. Per quanto riguarda l'attività esercitata da Scuole di Sci e Maestri di Sci, la questione più rilevante che interessa i minorenni riguarda la pubblicazione on – line, o comunque la diffusione, di immagini in formato fotografico o multimediale riguardanti minori d'età (per la quale si rinvia a pag. 30).

5 PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI – ARTT. 5, 6, 24 E 25 – REG. (UE) 2016/679

5.1 Accountability, Privacy by design, Privacy by default

I principi di accountability, privacy by design e by default, identificano il significato più profondo del nuovo sistema di protezione introdotto dal GDPR, nonché l'obbiettivo del presente documento. Il valore riconosciuto ai dati personali, quali elementi essenziali della vita privata, e pertanto idonei a rivelare informazioni caratterizzanti l'individuo, non consente di intraprendere la strada dell'adeguamento in modo passivo e superficiale.

Non è sufficiente dotarsi della modulistica prescritta, ma è indispensabile comprendere davvero ed avere consapevolezza della ragione di tali adempimenti: per questo si parla di ***Responsabilizzazione*** *(accountability, che più precisamente significa "dover rendere conto del proprio operato").*

Un rischio sostanziale per le aziende che recepiscono il GDPR è di concentrarsi sulla fase di raggiungimento del livello di conformità, trascurando l'esigenza (e l'opportunità) di intervenire sui processi aziendali, sulla competenza e la responsabilizzazione delle persone, nonché sul rafforzamento dei sistemi. Il Regolamento, infatti, richiede uno sforzo aggiuntivo, che si deve concretizzare nell'adozione di comportamenti proattivi volti a realizzare e dimostrare la concreta (e non meramente formale) predisposizione di meccanismi aziendali di sensibilizzazione, valutazione, controllo e tutela, da applicarsi ai trattamenti esistenti ed a eventuali trattamenti futuri. Non è più sufficiente, quindi, un approccio formalistico, volto ad esempio ad ottenere il consenso quale base giuridica idonea a ricomprendere qualsiasi trattamento, ma viene sancita la responsabilità del Titolare di tutelare l'Interessato e l'intera società dai rischi impliciti nel trattamento, usando la diligenza del buon padre di famiglia.

Il concetto di **privacy by design** risale al 2010, già presente negli USA e Canada, e poi adottato nel corso della 32° Conferenza mondiale dei Garanti privacy. La definizione fu coniata da Ann Cavoukian, Privacy Commissioner dell'Ontario (Canada). Sinteticamente, dare attuazione al concetto esaminato significa anticipare la tutela, progettando la protezione del dato personale sin dal principio.

Ciò richiede di configurare sin dall'inizio il trattamento dei dati, unitamente ai probabili rischi connessi al medesimo, predisponendo in seguito misure finalizzate a calmierare i rischi riscontrati e a provenire le violazioni.

I fondamenti che reggono il sistema di *privacy by design* sono i seguenti:

- prevenire, non correggere;
- *privacy* incorporata nel progetto;
- massima funzionalità, in maniera da rispettare tutte le esigenze di processo;
- sicurezza durante tutto il ciclo del prodotto o servizio;
- visibilità e trasparenza del trattamento, in tutte le fasi operative;
- centralità dell'utente.

Infine, l'architettura così progettata deve porre l'interessato e i suoi diritti al centro, elaborando modelli organizzativi precisi e calmierati al singolo caso, che garantiscano:

- la piena conoscenza dei trattamenti effettuati e delle finalità di trattamento;
- una costante valutazione della proporzionalità, della necessità e della liceità dei trattamenti rispetto alle finalità perseguite;
- la continua valutazione dei rischi e delle criticità relative alla protezione dei dati personali individuati nei vari processi aziendali;
- la predisposizione di misure e procedure volte ad affrontare i rischi ed a dimostrare la conformità alle disposizioni vigenti;
- la revisione periodica e l'aggiornamento delle misure adottate;
- la documentazione delle procedure adottate e dei processi di valutazione operati.

Il principio della **privacy by default**, invece, prevede che, per impostazione predefinita (di default, appunto), le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste, e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti (minimizzazione).

5.2 Liceità, correttezza e trasparenza

L'art. 5 GDPR prevede che i dati debbano essere "*trattati in modo lecito, corretto e trasparente nei confronti dell'interessato*". Si tratta di aspetti strettamente interconnessi, e per questo se ne offre una trattazione unitaria. In particolare, il **principio di correttezza** impone la chiarezza delle informazioni rese all'interessato, sostenendo la necessità che l'informativa fornita a quest'ultimo sia tale da far comprendere in modo adeguato ed esaustivo non solo le modalità del trattamento, ma anche le sue conseguenze. Quindi, il principio di correttezza si traduce nel concetto di lealtà e trasparenza. La **trasparenza** è un requisito che completa la definizione di correttezza, e mira ad alimentare il rapporto di fiducia tra Interessato e Titolare. Secondo questo principio, le informative che danno conto dei trattamenti effettuati devono essere facilmente accessibili e comprensibili (in particolare quando

riguardano minori). Nella stesura delle stesse deve essere impiegato un linguaggio semplice, in modo che gli Interessati siano in grado di capire cosa accadrà ai loro dati, e quali sono i possibili rischi che si potrebbero verificare nel corso delle operazioni di trattamento. La trasparenza, quindi, riguarda non solo il contenuto delle informazioni, ma anche le modalità in cui l'informazione viene rivolta agli Interessati.
Questa operazione risulterebbe sicuramente più efficace se alla consegna dell'informativa l'interessato venisse accompagnato nella lettura del documento, attraverso una breve e semplice spiegazione dei contenuti, da parte dell'addetto.
Così facendo, non solo verrebbe integrato il requisito della trasparenza, ma si contribuirebbe certamente alla diffusione di buone pratiche in materia di *privacy*, anche verso i soggetti "non addetti ai lavori". In fondo, ognuno di noi ha interesse a che le informazioni che lo riguardano siano trattate in modo lecito, corretto e trasparente.
Il **principio di liceità** merita una considerazione ulteriore, giacché l'art. 6 GDPR si occupa nel dettaglio di dettare le condizioni di liceità del trattamento, e le diverse basi giuridiche indicate spesso costituiscono limitazione all'esercizio del diritto alla protezione dei dati personali. Un'indicazione rilevante emerge dall'art. 52 della Carta dei diritti dell'Unione Europea: "*Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui*". Per questo è fondamentale il principio di liceità: il trattamento deve essere conforme alla legge e perseguire uno scopo legittimo.

6 SANZIONI

L'aspetto più rilevante in ambito sanzionatorio è che oggi, alla luce del Regolamento, le sanzioni non discendono solo da eventuali violazioni causate dal mancato rispetto dei principi di base in materia di protezione dei dati personali, ma, in ossequio all' accountability, anche da violazioni causate dalla mancata ottemperanza agli obblighi che gravano sul Titolare. Infatti, quest'ultimo deve saper rendere conto dell'attività svolta in ordine alla protezione del dato personale, dimostrando di aver implementato un sistema di data protection adeguato. In presenza di un'anomalia, il Garante per la protezione dei dati personali può imporre al Titolare delle misure di natura correttiva, da attuare nell'immediatezza, compreso il potere di limitare, sospendere o addirittura bloccare i trattamenti. Inoltre, se la violazione comporta danni agli interessati, il Titolare e/o il Responsabile del trattamento, dovranno provvedere al risarcimento dei danni, materiali e morali. Infatti, la normativa europea prevede che "chiunque subisca un danno

materiale o immateriale causato da una violazione [...] ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento" (art. 82 GDPR).

La responsabilità, invero, potrà essere di natura contrattuale, extracontrattuale, amministrativa, ed anche penale, giacché lo Stato italiano ha introdotto sanzioni specifiche all'interno dell'ordinamento, in caso di delitti informatici e trattamento illecito di dati.

Pertanto, il quadro sanzionatorio che si delinea appare particolarmente complesso e diversificato. Le sanzioni per l'inosservanza delle regole in materia di privacy non si limiteranno a quelle introdotte dal Regolamento UE (che, già sole, possono arrivare fino a 10 milioni di euro, o fino al 2% del fatturato annuo globale dell'esercizio precedente per inosservanza degli obblighi del titolare del trattamento e del responsabile del trattamento e per inosservanza degli obblighi dell'organismo di controllo; fino a 20 milioni di euro, o fino al 4% del fatturato annuo globale, per inosservanza dei principi di base del trattamento, come prevede l'art. 83 GDPR), giacché il legislatore nazionale ha previsto delle violazioni specifiche, contenute nell'art. 166 del Codice della privacy, recentemente modificato dal d.lgs. 101/2018, punite alla stregua delle sanzioni amministrative previste dal Regolamento e sopra elencate. Nel codice, inoltre, sono previste anche ulteriori ipotesi illecito (artt. 167, 167 bis, 167 ter, 170, 171), alle quali si aggiungono i reati espressamente previsti dal Codice Penale (reati informatici e di trattamento illecito di dati), alcuni dei quali possono costituire reati – presupposto per l'applicazione del d.lgs. 231/2001 in materia di responsabilità amministrativa dell'ente.

Inoltre, vari sono i provvedimenti correttivi introdotti dal Regolamento all'art. 56 par. 2 lett. da a) ad h) e j), che prevedono anche l'intervento diretto sui trattamenti, situazione che potrebbe comportare l'interruzione di un servizio verso i clienti, con evidente e immediato danno economico e reputazionale particolarmente rilevante.

In conclusione, si consideri che, all'art. 22, comma 13 del D.lgs. 101/2018, si legge: "Per i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie"; il che non significa che l'attività ispettiva è sospesa, ma soltanto che l'Autorità di controllo sarà più clemente nel primo periodo di cosiddetto – rodaggio.

ADEMPIMENTI PER ADEGUARSI AL GDPR E AL D.LGS. 101/2018

7 COME ADEGUARSI AL GDPR ED AL D.LGS. 101/18

Come già specificato, in applicazione del principio di responsabilizzazione (*accountability*) le Scuole di Sci ed il Maestro di Sci sono responsabili delle attività di trattamento svolte, in quanto Titolari del trattamento dei dati personali di clienti, dipendenti, collaboratori esterni, fornitori. Per questo motivo, diversi sono gli adempimenti richiesti dall'impianto normativo per costruire un sistema efficace di *data protection*. Tali operazioni sono suscettibili di adattamento da parte dei lettori in base alla propria realtà organizzativa, posto che l'elemento che deve guidare le procedure di adeguamento è l'analisi dei trattamenti eseguiti, i quali possono assumere connotazioni diversificate caso per caso.

7.1 Rispetto ed applicazione dei principi

I trattamenti devono apparire leciti, corretti, trasparenti, finalizzati allo scopo perseguito, ed inoltre devono rispondere alla prescrizione di accuratezza nella loro registrazione (i dati devono essere corretti, veritieri, completi, necessari e adeguatamente minimizzati). Inoltre, il Titolare deve definire idonee misure tecniche ed organizzative e, ove già presenti, verificarne l'attualità, a seguito di un'attività di analisi dei rischi affidata ad un esperto (ad esempio, con riferimento al sistema informatico, sarà necessario l'intervento di un tecnico, il quale dovrà predisporre un documento di sintesi in ordine al sistema IT utilizzato, alle eventuali misure di sicurezza implementate, ed agli eventuali rischi).

In generale, quindi, l'esercizio dei diritti degli interessati pone in capo al Titolare del trattamento una molteplicità di oneri che debbono essere adeguatamente gestiti attraverso la previsione di processi puntuali, definiti puntualmente nel registro dei trattamenti. Gli associati, quindi, dovranno dotarsi di tali misure organizzative.

7.2 Verificare la liceità del trattamento ai sensi dell'art. 6 GDPR

Il trattamento deve rientrare in almeno una delle condizioni di liceità previste dall'art. 6 GDPR, ed essere quindi sorretto da un'idonea base giuridica. In particolare, vengono identificate le seguenti condizioni, che devono essere indicate preventivamente nell'informativa rivolta all'interessato:

7.2.1 Consenso

Tra le varie basi giuridiche previste dall'art. 6, il consenso è la più significativa. La definizione di che cosa debba intendersi per consenso dell'avente diritto, è dettata all'art. 4, n.11. GDPR, secondo cui il consenso è rappresentato da: "*qualsiasi manifestazione di volontà libera, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante*

dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento".

Dalla nozione sopra citata, è possibile individuare i seguenti requisiti tipici del consenso dell'Interessato:

- LIBERTÁ: il consenso non deve essere indotto o suggerito. Ciò significa che l'interessato deve essere in grado di operare una scelta autenticamente libera, senza subire intimidazioni o raggiri, o più semplicemente limitazioni al rifiuto.

  In questo senso, la libertà del consenso è insussistente ove non sia possibile esprimere separatamente un assenso in relazione a distinti trattamenti di dati personali, oppure laddove l'esecuzione di un contratto venga subordinata alla dazione consenso in realtà non necessario a tale scopo.
- SPECIFICITÁ: il consenso deve essere raccolto per tutte le attività di trattamento svolte per la medesima finalità. Qualora il trattamento sottenda a più finalità, il consenso deve essere prestato in relazione a ciascuna di esse.
- INFORMATO: il consenso deve necessariamente fondarsi sulle informazioni contenute nell'informativa completa, predisposta dal Titolare del trattamento. Tuttavia, è bene sottolineare che il consenso spesso non è da ritenere affidabile, nel senso che poche persone in realtà prendono una decisione specifica, informata ed inequivocabile. Questo perché, purtroppo, pochi sono gli interessati che leggono attentamente le informative in materia. Questa base giuridica risulta sicuramente più efficace a legittimare il trattamento se, nella pratica, alla consegna dell'informativa l'addetto si adopera a spiegare brevemente il contenuto del documento che si chiede di firmare, in modo da evitare incomprensioni e dare efficacia al consenso. Infatti, rimane sempre la Responsabilità del Titolare di tutelare l'interessato e l'intera società dai rischi impliciti nel trattamento, creando appunto un sistema un'architettura di *data protection*.
- INEQUIVOCABILITÁ: il requisito della inequivocabilità del consenso si sostanza nell'assenza di dubbi riguardo al fatto che, col proprio comportamento, l'interessato abbia voluto operare quella precisa scelta autorizzativa.

  A tal fine, il comma 2 dell'art. 7 stabilisce che, qualora il consenso sia prestato nell'ambito di una dichiarazione scritta inerente anche ad altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie.
- VERIFICABILITÁ: il consenso non deve essere necessariamente documentato per iscritto, giacché è prevista la libertà della forma (anche se in alcune ipotesi -ad esempio dati sensibili - è necessario, in assenza di ulteriori condizioni di legittimità). Tuttavia, ove il trattamento sia fondato sul

consenso, l'associato deve essere in grado di dimostrare che l'interessato ha conferito tale consenso con riferimento allo specifico trattamento.

Si aggiunge che il consenso deve essere acquisito prima dell'inizio del trattamento e deve essere nuovamente raccolto in presenza di modifiche determinanti le caratteristiche, le finalità e le implicazioni del trattamento.

In via generale, il consenso non è prescritto laddove il trattamento sia fondato su basi giuridiche diverse (considerate dall'art. 6 GDPR, e spiegate nel prosieguo), come ad esempio il caso in cui il trattamento sia necessario a dare esecuzione a un contratto di cui l'interessato è parte, oppure per adempiere ad un obbligo legale al quale è soggetto il Titolare del trattamento.

Rispetto al trattamento dei dati particolari (sensibili) di cui all'art. 9 GDPR, anche in presenza delle condizioni sopra indicate, è consigliabile la raccolta di un consenso preventivo e specifico, specialmente in ragione del trattamento di dati sanitari del cliente (ad esempio, informazioni relative ad allergie o intolleranze alimentari se il Maestro si occupa del cliente per tutta la giornata, comprensiva anche del pranzo), salvo il caso in cui il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria, ovvero (solo in riferimento ai dati sanitari), che il trattamento sia necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso (art. 9 co. 2 l. c) GDPR), ad esempio in caso di infortunio.

Inoltre, il consenso è necessario anche quando si trattano dati biometrici intesi ad identificare in modo univoco una persona fisica (e quindi, fotografie e immagini video dove il soggetto è riconoscibile, e destinate alla diffusione, ad esempio, sui *social media*), soprattutto se si tratta di soggetti minorenni, inferiori degli anni 18, consenso che sarà, in questo caso, dato agli esercenti la Responsabilità genitoriale (meglio se entrambi).

Il consenso, infine, è necessario anche se si effettua attività di *marketing* (ad esempio mediante l'invio di *newsletter*), che prevede la trasmissione di comunicazioni commerciali circa l'attività, i servizi ed eventualmente i prodotti offerti (anche se per conto di terzi – ad esempio, noleggio di attrezzature sportive, attività commerciali organizzate quali asili nido ed escursioni, programma stagionale delle lezioni). Ogni contatto al quale si inviano simili informazioni deve aver fornito, a suo tempo, il consenso; se non è stato raccolto, è necessario informare circa la possibilità di recedere dal servizio, e procedere all'implementazione di idonee procedure a tal fine (ad esempio, *flag – in e out* sul sito web, per non autorizzare o revocare il consenso al servizio).

Si precisa che è compito del Titolare del Trattamento predisporre idonei moduli di consenso connessi all'informativa, rivolta principalmente a clienti e personale dipendente e collaboratore, i

quali dovranno essere strutturati separatamente per le specifiche finalità perseguite (e quindi con riferimento ad ogni singola categoria di dato particolare trattato), se si vorrà continuare a fare ricorso a tale base giuridica.

7.2.2 Adempimento di obblighi contrattuali

Il trattamento è lecito se è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso. Sostanzialmente, si tratta di una forma speciale di consenso. Nella specie, ad esempio, il trattamento dei dati anagrafici e bancari di clienti, dipendenti, fornitori e collaboratori della Scuola di Sci può essere sorretto da questa base giuridica, giacché senza di essi non si potrebbe dar luogo all'adempimento della relativa obbligazione contrattuale.

7.2.3 Obblighi di legge cui è soggetto il Titolare del trattamento

Nel caso di trattamento dei dati necessario per l'adempimento di obblighi derivanti da legge, regolamento o normativa comunitaria (come il trattamento per gli adempimenti fiscali e previdenziali) non occorre consenso.

7.2.4 Interessi vitali della persona interessata o di terzi

Il trattamento è ammesso se è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, come nel caso di un incidente avvenuto sulle piste da sci, oppure se l'interessato si trova nell'incapacità fisica di prestare il consenso (una persona si sente male mentre partecipa alla lezione, e quindi è possibile – e doveroso - trattare i suoi dati al fine di chiamare un'ambulanza). Si tratta, comunque, di una condizione di liceità residuale.

7.2.5 Legittimo interesse prevalente del Titolare o di terzi

Tale condizione di liceità interviene quando il trattamento è necessario per il perseguimento dei legittimi interessi del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

7.2.6 Interesse pubblico o esercizio di pubblici poteri

Il trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento (tramite legge statale o

dell'Unione) non richiede consenso, ma questo caso sicuramente non interessa la realtà della Scuola di Sci e del Maestro.

7.3 Informativa ai sensi dell'art. 13 D.lgs. 196/2003 e dell'art. 13 GDPR

Lo strumento dell'informativa, già previsto a livello interno dal 2003, con il GDPR si arricchisce di contenuti. Tale documento costituisce il cardine dell'impianto di *data protection* che ad ogni Titolare spetta di costruire: l'Interessato può effettivamente veder tutelati i suoi diritti, ed esercitarli, solo se è stato adeguatamente informato dal Titolare.

È opportuno che i Titolari di trattamento verifichino la rispondenza delle informative attualmente utilizzate ai criteri imposti dall'art. 13 GDPR, con particolare riguardo ai contenuti obbligatori e alle modalità di redazione, tenendo anche conto della presenza di dati particolari, in modo da apportare le modifiche o le integrazioni eventualmente necessarie ai sensi del Regolamento. Ancora con più urgenza, è necessario che si predispongano le diverse informative, ove mancanti (entro un mese dalla raccolta del dato). In generale, gli associati dovranno elaborare un'informativa diversa a seconda del trattamento effettuato, nonché della categoria di interessato.

La corretta stesura delle informative rende indispensabile la mappatura e il monitoraggio dei flussi; questa operazione consentirà di individuare con certezza le singole operazioni di trattamento interessanti i dati personali da parte della singola realtà, e di rispondere all'obbligo di rendere un'informazione esaustiva agli interessati dei cui dati si parla.

Pertanto, vanno predisposte singole informative differenziate in relazione ad ognuno degli interessati del trattamento (clienti, dipendenti, collaboratori, fornitori) in base alla categoria di dati trattati, ed inoltre va esibita un'adeguata *privacy policy* sul sito web, ove previsto.

In particolare, il Titolare deve specificare i dati di contatto del DPO (ove esistente), la base giuridica del trattamento, qual è il suo interesse legittimo se quest´ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti e garanzie (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello).

Il Regolamento prevede anche ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: in particolare, il Titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, nonché l'elencazione dei diritti che spettano all'interessato.

Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve altresì indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Gli esempi di informativa sono reperibili negli strumenti operativi, disponibili in conclusione al presente Vademecum (pag. 48).

7.4 Nomine ed organigramma funzionale

Il Titolare del trattamento ha il compito di monitorare il flusso dei dati all'interno dell'organizzazione e, a tal fine, individuare i soggetti che intervengono nel trattamento dei dati, definendone di conseguenza i compiti e le responsabilità con apposita nomina formale (si veda l'esempio riportato a pag. 59), come previsto in via generale dall'art. 2 – *quaterdecies* del d.lgs. 196/2003, così come innovato dal decreto dell'agosto 2018. Anche in presenza di un organigramma, è necessario aggiornare le nomine relative ai soggetti interni che trattano dati personali, con conseguente definizione di un organigramma ai fini *privacy*. Le figure da individuare sono quelle descritte nel par. 4.2 (pag. 11), e precisamente: Titolare, Autorizzato ed Interessato. Tale organigramma favorisce la suddivisione dei compiti in base alle competenze, e, nelle realtà più organizzate, consente l'individuazione di un referente per ogni area di trattamento. Tale ultimo adempimento non è previsto dalla normativa, ma rappresenta un'opportunità per garantire un adeguato monitoraggio dei trattamenti. Inoltre, in questa fase è fondamentale individuare i soggetti destinatari della comunicazione dei dati personali come Responsabili del trattamento (che si distinguono da eventuali sub – Responsabili, nominati dal Responsabile per l'esecuzione di specifiche finalità di trattamento per conto del Titolare del trattamento ai sensi dell'art. 28 co. 2 e 4 GDPR, cfr. par. 4.2.2). Gli specifici trattamenti da parte di un Responsabile devono essere disciplinati attraverso un contratto o altro atto giuridico a norma del diritto europeo, che riporti i contenuti essenziali sanciti all'art. 28 GDPR (si rimanda all'esempio di nomina riportato negli strumenti operativi, pag. 61). L'associato dovrà dotarsi di procedure organizzative e tecniche che consentano di valutare e di monitorare nel tempo l'operato dei Responsabili del trattamento in termini di conformità e rispondenza alle disposizioni vigenti in materia di protezione dei dati, nonché agli obblighi contrattuali derivanti dalla nomina (es. programmazione di *audit* periodici, redazione di report, etc.). Ogni misura e procedura a ciò preposta dovrà essere puntualmente documentata.

7.5 Registro dei trattamenti

L'art. 30 GDPR pone l'obbligo di tenuta del registro dei trattamenti in capo alle imprese e alle organizzazioni che impiegano un numero superiore a 250 dipendenti, o che svolgano attività di trattamento rischiose per i diritti e le libertà degli interessati, oppure trattamenti non occasionali, o inclusivi di categorie particolari di dati di cui all'articolo 9, paragrafo 1 GDPR, o ancora trattamenti di dati personali relativi a condanne penali e a reati di cui all'articolo 10 del Regolamento. Essendo questi casi che

interessano il caso di specie, giacché gli associati eseguono trattamenti non occasionali su dati personali, anche riferibili a particolari categorie di dati, è obbligatoria la tenuta del registro. In ogni caso, anche laddove vengano trattati solamente dati comuni, è fortemente consigliata la detenzione del registro, in quanto consente la mappatura dei flussi che interessano i dati personali presenti in azienda, rappresenta uno strumento indispensabile per monitorare le attività di trattamento e conseguentemente consentirne una corretta gestione. Un esempio di registro dei trattamenti è riportato a pag. 65.

7.6 Implementazione di misure di sicurezza adeguate

È necessario procedere alla definizione di idonee misure di sicurezza, ad integrazione quelle minime eventualmente già esistenti, così da raggiungere il requisito dell'adeguatezza di cui all'art. 32 GDPR. L'attività indicata non può prescindere dalla conduzione di una preventiva analisi dei rischi.

L'analisi dei rischi ha ad oggetto l'attività aziendale, lo spazio fisico in cui questa si esplica, ed in ultimo il sistema informatico. Ciò consente di individuare criticità e vulnerabilità, che vengono esplicate in un documento programmatico che da esito dei rilievi ottenuti e degli adempimenti necessari per garantire la protezione dei dati personali.

Ad esempio, è opportuno considerare le modalità di conservazione dei dati raccolti (informatica e/o cartacea), ed il luogo ove i dati si trovano (armadietti chiusi a chiave o scaffali liberamente accessibili, server interno o server in cloud). Inoltre, l'analisi riguarda anche le misure di salvaguardia dei dati stessi (antivirus, firewall, backup del server e dei sistemi gestionali utilizzati, accessi personalizzati con password, ecc.).

In particolare, è importante sottolineare che l'individuazione di criticità e vulnerabilità, esplicate in un documento programmatico, e soprattutto la valutazione circa l'efficacia delle misure di sicurezza adottate, dev'essere effettuata da un soggetto terzo al Titolare o al Responsabile del trattamento, così da garantire l'imparzialità della valutazione, ed evitare un conflitto di interessi.

A tal proposito, per quanto riguarda l'aspetto della protezione dei dati, è stata individuata la figura del "valutatore privacy", che può anche coincidere con quella del DPO, proprio per garantire un'analisi neutra del sistema di sicurezza con riferimento alla conformità delle policies aziendali rispetto al nuovo Regolamento (Norma UNI 11697/2017).

Pertanto, è opportuno affidare la valutazione circa l'efficacia delle misure di sicurezza ad un soggetto terzo e qualificato (valutatore privacy o DPO), che opera anche con il supporto di tecnici terzi (ad esempio, per l'analisi del sistema IT, il tecnico informatico).

7.7 Implementazione di procedure volte a gestire una violazione

Il Titolare del trattamento ha l'obbligo di documentare qualsiasi violazione dei dati personali subita, dando atto delle circostanze che hanno causato la violazione, delle conseguenze stimate e verificatesi nonché dei provvedimenti adottati per porvi rimedio.

Si rende pertanto necessaria la strutturazione di un registro delle violazioni volto a documentare le violazioni subite nei termini anzidetti sul modello indicato a pag. 67.

Andrà inoltre formalizzata una procedura di valutazione dei rischi volta a verificare se la violazione presenti un rischio per i diritti e le libertà degli interessati i cui dati sono stati violati, e che consenta poi di procedere alle comunicazioni prescritte agli artt. 33 (con riferimento all'autorità di controllo) e 34, par. 1 (in relazione al singolo interessato), GDPR.

7.8 Attività di formazione in materia di privacy

Ai sensi dell'art. 32 par. 4 GDPR, chiunque agisce sotto l'autorità del Titolare del trattamento e abbia accesso ai dati personali, non può trattare tali dati se non è istruito in tal senso dal Titolare stesso. Ciò sancisce espressamente un obbligo di formazione in capo al Titolare del trattamento verso gli autorizzati al trattamento a qualsiasi livello di inquadramento aziendale.

Tale formazione dovrebbe essere finalizzata ad illustrare i rischi generali e specifici dei trattamenti di dati, le misure organizzative, tecniche ed informatiche adottate, nonché eventuali responsabilità e sanzioni.

In questo senso, la formazione costituisce una misura di sicurezza per le organizzazioni, un onere a carico del Titolare, un diritto e un dovere per i dipendenti e i collaboratori, che dev'essere oggetto di una precisa pianificazione documentata. Inoltre, si tratta di un'attività utile alla creazione di una vera e propria "*cultura privacy*", per sensibilizzare gli operatori circa l'importanza e la delicatezza che questo tema ha assunto al giorno d'oggi.

Si suggerisce, pertanto, di predisporre un documento che renda conto delle pratiche e degli appuntamenti di formazione previsti per gli autorizzati al trattamento, nonché la predisposizione di *policy* aziendali che definiscano precise istruzioni operative per le attività di trattamento a cui gli stessi vengono preposti.

8 IN PRATICA...

È importante considerare che la normativa esaminata dal presente Vademecum richiede l'adozione di misure tecniche ed organizzative che consentano la gestione della *privacy* nel tempo.
Pertanto, ogni Associato dovrà adempiere, con un'azione dedicata, a quanto previsto dal regolamento, attenendosi alle presenti linee guida emanate da AMSI nazionale.

8.1 ANALISI dei TRATTAMENTI

In generale, nell'attività svolta dall'Associato, i trattamenti rilevanti ai fini privacy interessano principalmente dati di clienti, dipendenti, collaboratori, Maestri di sci associati e fornitori (cfr. cap. 3, pag. 7). In seguito, verranno analizzati i singoli processi, da un punto di vista pratico, e le relative linee di azione specifiche alle quale deve attenersi l'Associato.

8.1.1 I dati relativi al cliente

- Quali dati tratta l'Associato nell'ambito del suo rapporto con il cliente?

  La Scuola di Sci, nonché il singolo Maestro di Sci che lavora in autonomia, trattano quotidianamente, nell'ambito della propria attività, dati personali (comuni e particolari) dei clienti che vogliono usufruire delle lezioni di sci e dei vari servizi offerti. In particolare, tali dati (riferiti a soggetti maggiorenni e minorenni) possono essere:

- COMUNI: informazioni anagrafiche, di contatto, bancarie.
- PARTICOLARI: informazioni relative allo stato di salute (disabilità, intolleranze alimentari, allergie), materiale fotografico o video idoneo ad identificare in modo univoco un soggetto, dati relativi ad infortuni, informazioni razziali, etniche, di appartenenza linguistica o religiosa.

- L'Associato deve eseguire formalità particolari nel trattamento di tali dati?

  SI. Di ogni trattamento dev'essere data informazione all'interessato: a tal fine viene utilizzato il principale strumento dell'**informativa**, la quale ovviamente dovrà differenziarsi a seconda dei servizi offerti, ed inoltre prevedere il consenso quando necessario per la legittimità del trattamento. In particolare, il **consenso** DEVE essere richiesto:

  - per finalità di marketing (invio di comunicazioni commerciali, newsletter);
  - per la diffusione di immagini (foto, video) su siti web e/o social network o altro canale di comunicazione (TV), specialmente se si tratta di soggetti minori degli anni 14;
  - per il trattamento di particolari categorie di dati, come quelli sanitari.

Inoltre, è consigliabile la tenuta del **registro dei trattamenti**, giacché l'Associato effettua trattamenti non occasionali su dati personali, anche riferibili a particolari categorie di dati. Tale strumento, consente la mappatura dei flussi che interessano i dati personali presenti in azienda, e riferiti al cliente, e quindi rappresenta uno strumento indispensabile per monitorare le attività di trattamento e conseguentemente consentirne una corretta gestione.

- Ci sono delle regole particolari in caso di raccolta e diffusione di immagini?

  Si. Occorre fare particolare attenzione nel pubblicare immagini, soprattutto se riguardano soggetti minorenni. L'articolo 10 del Codice Civile italiano dispone che *qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia esposta, o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni*. La normativa nazionale di riferimento è proprio la Legge sul diritto d'autore (L n. 633/1941 e successive modifiche), che stabilisce i limiti alla pubblicazione dei ritratti, alla quale si deve aggiungere la normativa sulla *privacy*. Il concetto di base è espresso nell'articolo 96 della L. sul diritto d'autore, che recita: *il ritratto di una persona non può essere esposto, riprodotto e messo in commercio senza il consenso di questa*, salvo quanto previsto dall'art. 97, il quale chiarisce che *non occorre il consenso della persona ritrattata quando la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali o quando la riproduzione è collegata ad avvenimenti, cerimonie di interesse pubblico svoltisi in pubblico. Il ritratto non può tuttavia essere esposto, o messo in commercio, quando l'esposizione o messa in commercio rechi pregiudizio all'onore, alla reputazione o anche al decoro della persona ritrattata*. Invero, il volto di una persona ritratto in una fotografia, o riprodotto in un video, è considerato dato personale, per cui è necessaria una menzione a riguardo nell'**informativa** privacy di cui all'art. 13 GDPR, volta ad ottenere il **consenso specifico** (cd. liberatoria) per la diffusione dello stesso, specialmente se ci si riferisce a soggetti minorenni (inferiori degli anni 18), che sarà in questo caso rivolta agli esercenti la Responsabilità genitoriale (meglio se entrambi).

  Ovviamente, se il volto non è riconoscibile, non sussiste problema di *privacy* e l'immagine può essere pubblicata senza alcuna autorizzazione, così come nell'ipotesi in cui si rappresenti in foto o video un luogo pubblico o aperto al pubblico oppure un evento, e i personaggi vengono ritratti accidentalmente (sebbene siano riconoscibili). In sostanza, la persona ritratta deve poter essere eliminata senza che la foto o il video perda la sua autonomia. Questo vale anche se delle persone

è ritratta una parte del corpo, poiché la *privacy* in questo ambito riguarda la riconducibilità del dato biometrico ad una persona specifica, individuata o individuabile, e quindi riconoscibile, caratteristica che è legata al volto e non a particolari anatomici, pure se peculiari.

- Come e per quanto tempo devono essere conservati tali dati?

  L'Associato deve definire una politica di durata e conservazione del dato, e darne conto sia nell'informativa, che nel registro dei trattamenti. In particolare, è necessario sviluppare un sistema conservazione dei dati che sia idoneo a garantirne l'integrità e la riservatezza. Alcuni suggerimenti:
  - Conservazione cartacea: in maniera sistematica ed ordinata ed in luogo sicuro, meglio se in armadietto chiuso a chiave;
  - Conservazione elettronica: su server o gestionale installato sulla macchina, dotato di procedure di backup frequenti, protetto con antivirus e firewall.

  Lo smaltimento di tali dati deve avvenire entro i termini di legge, ovvero nel momento in cui gli stessi non sono più necessari per l'adempimento delle finalità previste. In genere, per la normale amministrazione, tale periodo si identifica in 10 anni (che possono aumentare se richiesto da finalità contributive, fiscali, di accertamento o giudiziarie).

- Cosa deve fare l'Associato in caso di INFORTUNIO?

  Se avviene un infortunio durante l'attività elargita dall'Associato al cliente, qualsiasi ne sia la causa, il Maestro è tenuto a redigere un verbale contenente i dati (anche sanitari) relativi al cliente. Tali informazioni, poi, vengono comunicate ad un soggetto terzo, ovvero l'assicurazione, ed eventualmente utilizzate in sede giudiziaria.

  Si consideri che l'informazione sanitaria relativa all'infortunio dev'essere trattata con maggiore cautela, e nel rispetto delle prescrizioni legali. Non vi dev'essere diffusione alcuna (salvo per quanto riguarda le comunicazioni a terzi, come l'intermediario assicurativo, per le quali si parla appunto di comunicazione, e non di diffusione), e la conservazione deve essere maggiormente attenta alla riservatezza e all'integrità del dato (in cartelle apposite, conservate in luogo sicuro).

...RIASSUMENDO:

Adempimenti relativi ai dati relativi al CLIENTE
☐ Predisporre l'**informativa**, consegnarla e farla firmare dal cliente al momento della raccolta dei dati.

☐ Chiedere il **consenso specifico**, in calce all'informativa, per finalità di marketing (invio di comunicazioni commerciali, newsletter), per la diffusione di immagini (foto, video) su siti web e/o social network o altro canale di comunicazione (TV), per il trattamento di particolari categorie di dati, come quelli sanitari. ☐ Se ci si riferisce a immagini o video ritraenti soggetti minorenni, il consenso sarà rivolto agli esercenti la Responsabilità genitoriale (entrambi).
☐ Compilare il **registro dei trattamenti**.
☐ Trattare i dati particolari (ad esempio quelli sanitari) in modo sicuro ed adeguato.
☐ Smaltire i dati non più necessari.

8.1.2 I dati relativi ai dipendenti, ai collaboratori ed agli Associati

In questa sezione si considera la realtà propria delle Scuole di Sci, che esercitano la loro attività dotandosi di una struttura associativa più o meno organizzata. Infatti, la Scuola effettua trattamenti anche di dati dei dipendenti (ad esempio, del personale di segreteria o dei maestri assunti), nonché dei maestri operanti in regime di P.IVA, ed infine dei Maestri che, sebbene non esercitino la loro professione con la Scuola, sono associati alla stessa.

- Quali dati tratta la Scuola nell'ambito del suo rapporto con il dipendente, il collaboratore, l'associato?

  All'interno della Scuola di Sci si possono registrare trattamenti su dati:

  - COMUNI: informazioni anagrafiche, di contatto, bancarie, numero della licenza ed attestazione dell'iscrizione all'albo;
  - PARTICOLARI: dati relativi ad infortuni sul lavoro, materiale fotografico o video idoneo ad identificare in modo univoco il soggetto, dati relativi a condanne penali o reati (in particolare, ai sensi dell'art. 2 d.lgs. 39/2014, in attuazione della Direttiva 2011/93/UE, tutti i datori di lavoro pubblici e privati l'obbligo di richiedere il certificato penale del casellario giudiziale per gli addetti – assunti o in collaborazione, anche volontaria – che hanno contatti diretti e regolari con i minori).

  Se si svolgono procedure di selezione del personale (colloqui), è importante limitarsi a raccogliere solo le informazioni utili a determinare l'idoneità alla mansione, evitando quindi di indagare su aspetti personali del candidato (ad esempio, opinioni politiche o dichiarazioni di appartenenza sindacale, razziale, etnica).

- La Scuola deve eseguire formalità particolari nel trattamento di tali dati?

  A livello interno, è certamente importante informare l'interessato circa i trattamenti che riguardano i suoi dati personali, effettuati da parte della Scuola di Sci, mediante un'apposita **informativa**, da allegare al contratto. Se si ritiene di dover pubblicare foto o video che ritraggono l'interessato, è opportuno chiedere il **consenso** specifico in calce all'informativa. Inoltre, appare fondamentale effettuare la **nomina ad Autorizzato al Trattamento dei dati**, se il dipendente, il maestro assunto o collaboratore esegue trattamento di dati personali relativi a clienti e/o altri dipendenti o collaboratori, giacché la Scuola è Titolare di quei dati, e nell'esercizio delle sue attività si avvale di soggetti che eseguono trattamenti sui dati raccolti in quanto Titolare (nel dettaglio si veda il modello predisposto e disponibile negli strumenti operativi, pag. 59). Tali soggetti, infatti, sono veri e propri Autorizzati al Trattamento, ai sensi dell'art. 4 GDPR (cfr. par. 4.2.5., pag. 14), e come tali devono essere destinatari di apposita nomina formale, nonché di specifica **formazione** ai fini privacy. Tutto ciò, inoltre, deve essere documentato nel **Registro dei trattamenti**.

- La scuola può controllare l'attività del dipendente, del collaboratore, o dell'associato?

  Alcuni associati possono essersi dotati di un sistema di videosorveglianza. Questa attività introduce rilevanti questioni giuslavoristiche. Infatti, ai sensi dell'articolo 4 della Legge n. 300/1970 (Statuto dei Lavoratori) *è proibito l'utilizzo di sistemi di videosorveglianza e di qualsiasi altro dispositivo che consenta il controllo a distanza dei lavoratori* (come ad es. geolocalizzazione), salvo che:

  a) i dispositivi siano necessari per esigenze organizzative, tecniche e produttive o per la salute e la sicurezza dei lavoratori o per proteggere il patrimonio aziendale;

  b) prima dell'installazione dei dispositivi, sia siglato un accordo con le rappresentanze sindacali in merito all'utilizzo di tali dispositivi o (in mancanza di accordo) previa autorizzazione dell'Ispettorato Territoriale del Lavoro (salvo che siano necessari per registrare la presenza dei lavoratori nei luoghi di lavoro, ovvero siano utilizzati dai lavoratori per lo svolgimento della prestazione);

  c) siano rispettati i requisiti richiesti dalla normativa in materia di protezione dei dati personali.

  Nelle attività di sorveglianza, quindi, occorre rispettare il divieto di controllo a distanza dell'attività lavorativa, e pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul badge).

Secondo la giurisprudenza (Corte di Appello di Milano, 30 settembre 2005, Tribunale di Milano, 31 marzo 2004, Corte di Cassazione, 12 febbraio 1983, n. 1236), il concetto di controllo a distanza ha sia una dimensione spaziale che temporale, giacché costituisce controllo a distanzia sia il controllo da remoto, all'insaputa dei lavoratori, sia il controllo svolto in presenza dei lavoratori su azioni da essi compiute nel passato. Entrambi i casi costituiscono un controllo a distanza ai sensi dell'articolo 4 dello Statuto dei Lavoratori.

Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro. In tali casi, ai sensi dell'art. 4 della l. n. 300/1970, gli impianti e le apparecchiature, *dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti* (v., altresì, artt. 113 e 114 del Codice; art. 8 L. n. 300/1970 cit.; art. 2 d.lgs. n. 165/2001).

Come emerge chiaramente dal Provvedimento in materia di videosorveglianza, emesso dal

Garante per la protezione dei dati personali (all. 2), in ogni caso, gli Interessati (clienti, dipendenti, collaboratori, Maestri associati e fornitori) devono essere sempre informati che stanno per accedere ad una zona videosorvegliata. A tal proposito, connotato da elementi di novità si delinea il par. 7 dell'art. 12 GDPR, con il previsto richiamo alla possibilità di rendere le informazioni di cui agli artt. 13 e 14 GDPR in combinazione con icone standardizzate, anche presentate elettronicamente. Su tale previsione si appunta chiaramente la volontà del legislatore europeo di coniugare trasparenza nei fini ed efficacia dei mezzi, agevolando la veicolazione e la facile comprensione delle informazioni. Tuttavia, come rilevato dal WP29 (il gruppo di lavoro in materia di protezione dei dati personali), il ricorso all'utilizzo di icone non dovrebbe essere inteso nei termini di una semplice sostituzione delle informazioni da fornire all'interessato, posto che la *ratio* di tale previsione è, piuttosto, quella di aumentare la chiarezza per gli interessati, riducendo il ricorso ad ingenti quantità di informazioni scritte.

Pertanto, la segnalazione agli utenti deve essere effettuata tramite appositi cartelli, collocati a ridosso dell'area interessata, ed in modo tale che risultino chiaramente visibili.

Nel caso in cui i sistemi siano attivi durante le ore notturne, i cartelli devono essere opportunamente illuminati. Essi devono inoltre contenere un simbolo o un'immagine stilizzata di semplice comprensione che rimandi all'uso di telecamere, il nominativo dei soggetti che hanno accesso alle strumentazioni e alla visualizzazione delle immagini riprese, ed un riferimento all'informativa completa (redatta ai sensi dell'art. 13 GDPR), la quale deve essere facilmente accessibile con strumenti informatici (ad esempio, pubblicazione sul sito internet), e fisici (come l'affissione in bacheca, presso il punto informazioni). Nel caso del personale dipendente, invece, è bene inserire un richiamo al sistema di videosorveglianza nell'apposita informativa, che viene consegnata al momento dell'assunzione.

- Come e per quanto tempo devono essere conservati tali dati?

  Ugualmente a quanto avviene per i dati del cliente, l'Associato deve definire una politica di durata e conservazione del dato relativo al dipendente / collaboratore, e darne conto sia nell'informativa, che nel registro dei trattamenti. In particolare, è necessario sviluppare un sistema conservazione dei dati che sia idoneo a garantirne l'integrità e la riservatezza, allo stesso modo di quanto è già stato suggerito con riguardo al cliente (ed anche in maniera più accorta, visto la delicatezza di alcuni dati trattati, come quelli relativi al casellario giudiziale).

  Lo smaltimento di tali dati deve avvenire entro i termini di legge, ovvero nel momento in cui gli stessi non sono più necessari per l'adempimento delle finalità previste. In particolare, per le attività di amministrazione (contabilità, gestione paghe, formazione del personale), contrattuali e giuslavoristiche, nonché di gestione dell'eventuale contenzioso, la conservazione deve avvenire per un tempo di conservazione pari nel massimo a 10 anni, come stabilito per legge dal disposto di cui all'art. 2220 C.C. Per quanto riguarda la videosorveglianza, invece, il termine massimo di conservazione dell'immagine è sancito in 7 giorni.

- Cosa deve fare l'Associato in caso di INFORTUNIO?

  I dati relativi all'infortunio possono riguardare anche dipendenti, collaboratori, o Maestri associati. Di tali dati la Scuola deve garantire particolare riguardo, in ragione della loro delicatezza. Non vi dev'essere diffusione alcuna (salvo per quanto riguarda le comunicazioni a terzi, come l'intermediario assicurativo, o l'INAIL, per le quali si parla appunto di comunicazione e non di

diffusione), e la conservazione deve essere maggiormente attenta alla riservatezza e all'integrità del dato (in cartelle apposite, conservate in luogo sicuro).

…RIASSUMENDO:

Adempimenti relativi a DIPENDENTI; COLLABORATORI; ASSOCIATI
☐ Predisporre l'**informativa**, consegnarla e farla firmare dall'interessato al momento della raccolta dei dati (stipula del contratto).
☐ Chiedere il **consenso specifico**, in calce all'informativa, per la diffusione di immagini (foto, video) su siti web e/o social network o altro canale di comunicazione (TV), e per il trattamento di particolari categorie di dati, come quelli sanitari relativi all'infortunio sul lavoro.
☐ Compilare il **registro dei trattamenti**.
☐ Trattare i dati particolari (ad esempio quelli relativi all'infortunio sul lavoro) in modo sicuro ed adeguato e verificare che i dati raccolti non siano eccessivi rispetto alla finalità del trattamento.
☐ Smaltire i dati non più necessari.
☐ Predisporre le dovute **nomine ad Autorizzato al trattamento** rivolte ai soggetti interni che eseguono trattamento di dati su indicazione del Titolare del Trattamento (ad esempio, il personale di segreteria).
☐ Adempiere all'obbligo di **formazione** in materia di *privacy* rivolto ai soggetti che eseguono trattamenti di dati personali all'interno dell'Associazione.

8.1.3 I dati relativi ai fornitori

L'Associato, e specialmente la Scuola di Sci, in quanto realtà organizzata e strutturata, intrattiene rapporti che interessano dati personali anche con soggetti esterni all'Associazione.
Inoltre, vi può essere esternalizzazione dei dati dei clienti, dei dipendenti e dei collaboratori, ad esempio, a fornitori di servizi, quali commercialista, consulente del lavoro, assicurazione, servizio legale, fotografo, videomaker, tecnico informatico, tecnico o soggetto che gestisce il sito web e l'area social media.

- Quali dati tratta l'Associato nell'ambito del suo rapporto con il fornitore?
  Relativamente ai fornitori, si può registrare la presenza di dati:
  - COMUNI: informazioni anagrafiche, di contatto, bancarie.

- L'Associato deve eseguire formalità particolari nel trattamento di tali dati?

Innanzitutto, è importante informare l'interessato circa i trattamenti che riguardano i suoi dati personali, effettuati da parte dell'Associato, mediante un'apposita **informativa**, da allegare al contratto. Dal momento che, generalmente, si trattano solo dati comuni e per finalità di esecuzione contrattuale, non serve il consenso specifico.

Se il fornitore presta dei servizi che riguardano dati appartenenti al Titolare, tuttavia, si registra una fuoriuscita di dati. Pertanto, è fondamentale elaborare una **nomina a Responsabile del trattamento** ai sensi dell'art. 28 GDPR, che funge da vero e proprio contratto (accordo tra le parti) in ordine al trattamento di dati personali effettuato dal soggetto terzo per conto dell'Associato. Il fornitore, infatti, per poter prestare il servizio, deve necessariamente eseguire trattamenti sui dati del Titolare (ovvero l'Associato), e relativi a clienti, dipendenti, collaboratori, associati e altri fornitori. Ad esempio, il videomaker, nel realizzare il video promozionale su incarico della Scuola di Sci, conserverà ed utilizzerà le immagini dei bambini che hanno partecipato ai corsi di sci (s'intende, solo dei bambini i cui genitori hanno espressamente autorizzato tale trattamento). Ebbene, è chiaro che il Titolare non può rispondere per eventuali violazioni causate dal fornitore esterno (si tratterebbe, altrimenti, di una sorta di responsabilità oggettiva). Tornando all'esempio di prima, sarebbe ingiusto pensare che la singola Scuola di Sci che ha commissionato la realizzazione del video dovesse rispondere, sempre e comunque, del fatto che il videomaker abbia pubblicato illegalmente, in rete, i contenuti dei bambini, oppure abbia subito un attacco informatico dovuto alle scarse misure di sicurezza, o, ancora, abbia perso tutte le immagini perché dotato di un carente sistema di backup. È per questo che è fondamentale elaborare un accordo formale tra Titolare (nella specie Scuola di Sci o singolo Maestro), e fornitore (ad esempio, il videomaker), che definisca con precisione la natura e le finalità del trattamento, nonché le relative modalità e la base giuridica (adempimento di un obbligo contrattuale, con richiamo al singolo contratto stipulato tra le parti), la durata del trattamento (con indicazione delle modalità di conservazione a fine rapporto, se prevista), gli obblighi del Responsabile e le misure di sicurezza garantite dallo stesso, compresa l'autorizzazione da parte del Titolare di nominare sub - Responsabili (nel dettaglio si veda il modello predisposto e disponibile negli strumenti operativi, pag. 61). Il documento, elaborato in collaborazione tra le parti, costituirà un vero e proprio contratto, che va ad integrare quello già presente tra le parti per la fornitura del singolo servizio. Più dettagliata sarà tale nomina, più definiti saranno i confini delle responsabilità delle parti in ordine ad eventuali violazioni ai diritti dell'Interessato.

Inoltre, di tale nomina se ne deve dar conto nell'informativa destinata al singolo interessato, giacché si tratta di comunicazione del dato a soggetto terzo (destinatario).

Tutto ciò, inoltre, deve essere documentato nel **Registro dei trattamenti**, registro che dev'essere tenuto anche dal fornitore, in qualità di Responsabile del trattamento.

- Come e per quanto tempo devono essere conservati tali dati?
  Anche in questo caso, l'Associato deve definire una politica di durata e conservazione del dato relativo al fornitore, e darne conto sia nell'informativa, che nel registro dei trattamenti. In particolare, è necessario sviluppare un sistema conservazione dei dati che sia idoneo a garantirne l'integrità e la riservatezza, alla stregua dei suggerimenti sopra espressi.
  Come sopra, lo smaltimento di tali dati deve avvenire entro i termini di legge, ovvero nel momento in cui gli stessi non sono più necessari per l'adempimento delle finalità previste.

…RIASSUMENDO:

Adempimenti relativi ai FORNITORI
☐ Predisporre l'**informativa**, consegnarla e farla firmare per presa visione dall'interessato al momento della raccolta dei dati (stipula del contratto).
☐ Compilare il **registro dei trattamenti**.
☐ Smaltire i dati non più necessari.
☐ Predisporre le dovute **nomine a Responsabile del trattamento** rivolte ai soggetti esterni che eseguono trattamento di dati per conto del Titolare del Trattamento.

8.1.4 Il sito web e i social media

Un discorso a parte merita la gestione del sito web utilizzato dall'Associato per finalità pubblicitarie, di marketing diretto, e/o informative.
In particolare, i problemi in merito alla *privacy* sorgono nel momento in cui il sito web consente la raccolta di dati personali (ad esempio, mediante un questionario, una semplice consultazione, un modulo di contatto, oppure un form di pubblicazione contenuti vari, quali le recensioni del cliente, o ancora tramite la creazione di un account specifico).

- Quali dati tratta l'Associato nell'ambito del suo rapporto con l'utente del sito web?
  Qualora il sito web permetta l'inserimento di dati personali (riferiti a soggetti maggiorenni e minorenni), si può verificare il trattamento di dati comunicati volontariamente dall'utente, che si riferiscono, generalmente, ad informazioni anagrafiche e di contatto (dati COMUNI).

Non solo: con il sito web, l'Associato raccoglie anche dati di navigazione (cookies), per finalità di analisi statistica (in forma esclusivamente aggregata e anonima), e/o per finalità di sicurezza, o ancora per attività accessorie (funzioni necessarie o strumentali all'operatività del servizio, anche per mezzo di soggetti terzi, come ad esempio il *web hosting*). I cookies, infatti, permettono di conservare informazioni sulle preferenze dei visitatori, e sono utilizzati al fine di verificare il corretto funzionamento del sito e migliorarne le funzionalità personalizzando il contenuto delle pagine in base al tipo del browser utilizzato, oppure per semplificarne la navigazione automatizzando le procedure (es. login, lingua sito), ed infine per l'analisi dell'uso del sito da parte dei visitatori.

- L'Associato deve eseguire formalità particolari nel trattamento di tali dati?

  SI. Sul sito web dev'essere garantita una corretta informazione all'interessato: a tal fine, viene utilizzato il principale strumento della **web policy**, la quale ovviamente dovrà dare conto dei vari trattamenti effettuati e fornire tutte le informazioni richieste dagli artt. 13 e 14 GDPR, ed inoltre prevedere il consenso quando necessario per la legittimità del trattamento. In particolare, il **consenso** DEVE essere richiesto per finalità di marketing (invio di comunicazioni commerciali, newsletter), mediante un apposito *flag – in* presente nel form dove l'utente inserisce i dati personali. Pertanto, se l'Utente non spunta la casella di consenso, non è possibile utilizzare i suoi dati (di contatto) per l'invio di informazioni commerciali e pubblicitarie, nemmeno in forma di newsletter. Inoltre, è importante esibire anche un'apposita **cookie policy**, giacché mediante i cookies si raccolgono file di testo, che vengono registrati sul terminale dell'utente, oppure che consentono l'accesso ad informazioni sul terminale dell'utente. Il **consenso** si manifesta anche in relazione ad alcuni *cookies*, giacché è data possibilità di rifiutare l'utilizzo dei cookies e revocare un consenso già fornito (con un apposito banner presente all'inizio della navigazione, oppure direttamente dal browser). In caso di cookie pubblicitari, cookie riferiti ai social network, cookie di terze parti e cookie che misurano gli accessi (e quindi che registrano dati di navigazione non anonimi), infatti, il consenso deve essere precedente alla lettura del contenuto del sito da parte dell'utente, e finché lo stesso non ha dato il suo consenso, i cookie non possono essere depositati o letti dal sito stesso.

  I processi che interessano la gestione del sito web – ove presente – e riferiti al trattamento di dati personali (forniti direttamente dall'utente e/o raccolti in modo automatizzato) devono essere considerati all'interno del **registro dei trattamenti**.

- Come e per quanto tempo devono essere conservati tali dati?

  L'Associato deve indicare, nella web policy e nella cookie policy, nonché nel registro dei trattamenti, la durata e la modalità di conservazione del dato.

  Infatti, i dati raccolti dal sito durante il suo funzionamento devono essere conservati per il tempo strettamente necessario a svolgere le attività precisate. Alla scadenza di tale termine, i dati saranno cancellati o anonimizzati, a meno che non sussistano ulteriori finalità per la conservazione degli stessi.

  In particolare, è fondamentale fornire l'indicazione circa la durata della conservazione delle informazioni relative all'indirizzo IP (non anonimizzate), utilizzate a fini di sicurezza del sito (blocco tentativi di danneggiare il sito).

…RIASSUMENDO:

Adempimenti relativi al SITO WEB
☐ Predisporre o aggiornare la **privacy policy** in base ai contenuti legali obbligatori.
☐ Chiedere il **consenso specifico**, per finalità di marketing (invio di comunicazioni commerciali, newsletter) – se previste - al momento dell'inserimento di dati da parte dell'Utente.
☐ Predisporre o aggiornare la **cookie policy.**
☐ Verificare la presenza di cookies e, se necessario, creare un banner di raccolta e revoca del **consenso specifico**.
☐ Inserire tale processo nel **registro dei trattamenti**.

8.2 ANALISI DEI RISCHI E MISURE di SICUREZZA.

Come già specificato più volte nel presente Vademecum, la nuova normativa europea punta tutto sulla **responsabilizzazione** del Titolare del Trattamento.

Per questo motivo, appare fondamentale – **caso per caso** - studiare ed implementare valide misure tecniche e organizzative modellate sulla singola realtà considerata. È l'adempimento richiesto dall'art. 32 GDPR, che si riferisce nello specifico alla sicurezza del trattamento di dati personali. Tenuto conto della *best available technology* dei costi (approccio pragmatico), dell'ambiente di trattamento dei dati, dei soggetti coinvolti, del perimetro di circolazione, del rischio (*asset* dato personale) e del bene giuridico tutelato (diritto alla privacy e alla tutela dei dati personali) occorre attuare misure adeguate.

L'attività sopra indicata non può prescindere dalla conduzione di un'attività di analisi dei rischi. Tale analisi deve riguardare tutti i trattamenti e i luoghi di lavoro, nonché i dispositivi fisici e remoti (documentazione cartacea, server, software, etc.) dove sono conservati i dati personali, e mira a rilevare le potenziali minacce alla sicurezza, riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento.

Normalmente, la valutazione circa l'efficacia delle misure di sicurezza adottate, è affidata ad un soggetto terzo al Titolare o al Responsabile del trattamento, così da garantire l'imparzialità della valutazione, ed evitare un conflitto di interessi.

Di seguito, si propongono buone prassi, a titolo esemplificativo e non esaustivo, per la sicurezza dei dati personali, da implementare nelle varie realtà che interessano le attività dell'Associato. L'azione dev'essere quella di seguire il dato durante il percorso che lo stesso compie sotto la Titolarità del Titolare del Trattamento, e stabilire *ex ante* i singoli processi e i vari adempimenti richiesti dall'impianto normativo (chi fa cosa, come, quando, fino a quando).

8.2.1 I dati in formato cartaceo

a) RACCOLTA

I dati personali vengono raccolti dall'Interessato in forma cartacea in diversi momenti: al momento del primo contatto con il CLIENTE che fisicamente si reca in ufficio, o presso il punto informativo sulle piste; al momento della stipula del contratto con il DIPENDENTE, il COLLABORATORE, o il FORNITORE, o ancora all'atto dell'iscrizione all'Associazione da parte del singolo MAESTRO di SCI.

b) CONSERVAZIONE

In questa fase, i rischi riguardano le seguenti circostanze:

- Presenza di persone non autorizzate;

- Furto di documentazione e/o strumentazione contenente dati;
- Eventi distruttivi di varia natura;
- Errori umani nella gestione della sicurezza (ad esempio, l'Associato si dimentica di chiudere a chiave il locale dove sono conservati i documenti).

È necessario, pertanto, implementare misure di sicurezza tecniche ed organizzative adeguate, ad esempio:

- MISURE ORGANIZZATIVE: Definizione di istruzioni chiare per il personale circa la conservazione, nel senso di archiviare in modo sistematico ed ordinato il documento (in cartelle organizzate); vincolare il personale alla riservatezza;
- MISURE TECNICHE: Protezione dei locali, ovvero conservare i documenti preferibilmente in armadietti chiusi a chiave e ignifughi, situati negli uffici amministrativi o comunque in luogo non accessibile al pubblico; dotazione di allarme antintrusione e sistema antincendio.

c) DISTRUZIONE

Il dato deve essere conservato per il tempo previsto dalla legge, ed inoltre devono essere trattati solo i dati necessari alla specifica finalità del trattamento. Ne consegue che i dati non più necessari e quelli non utili devono essere smaltiti, in base alle seguenti procedure:

- MISURE ORGANIZZATIVE: Definizione di istruzioni chiare per il personale, riguardanti la distruzione del dato, come ad esempio la revisione periodica dell'archivio (ogni 6 mesi, ogni anno), la selezione dei documenti "scaduti", ovvero che hanno superato il termine legale di conservazione (generalmente, 10 anni) e la conseguente eliminazione del dato cartaceo mediante apposita macchina distruggi documenti;
- MISURE TECNICHE: Dotazione di una macchina distruggi documenti.

8.2.2 I dati in formato elettronico

a) RACCOLTA

I dati personali vengono raccolti dall'Interessato in forma elettronica in diversi momenti: al momento del primo contatto con il CLIENTE che fisicamente si reca in ufficio, al momento della stipula del contratto con il DIPENDENTE, il COLLABORATORE, o il FORNITORE, o ancora all'atto dell'iscrizione all'Associazione da parte del singolo MAESTRO di SCI. o in un periodo successivo, trasferendo le informazioni dal modulo/contratto stipulato al gestionale utilizzato.

b) CONSERVAZIONE

Molte sono le problematiche riguardanti la strumentazione elettronica, perché sottoposta generalmente ad attacchi più probabili e frequenti, visto il continuo progresso tecnologico:

- Azione di virus;

- Spamming;
- Eventi distruttivi di varia natura;
- Errori umani nella gestione della sicurezza (ad esempio, perdita di credenziali di autenticazione).
- Malfunzionamento o degrado degli strumenti;
- Intrusione esterna (attacco informatico).

È fondamentale implementare valide misure di sicurezza tecniche ed organizzative, ad esempio:

- MISURE ORGANIZZATIVE: Adozione e implementazione di *policy* e procedure IT sulla sicurezza; sensibilizzazione del personale circa l'utilizzo del sistema informatico, specialmente per quanto riguarda le password, l'utilizzo della rete e l'uso dei documenti;
- MISURE TECNICHE: Dotazione di un sistema di autenticazione informatica (password personalizzate, con revisione periodica automatizzata, meglio se ogni 3 mesi), installazione di programmi antivirus aggiornati automaticamente su ogni macchina, firewall, backup frequente ed automatico, gruppo di continuità, sistema RAID, installazione di software sul server interno, implementazione di procedure di *disaster recovery*.

c) DISTRUZIONE

Il dato elettronico deve essere conservato per il tempo previsto dalla legge, ed inoltre devono essere trattati solo i dati necessari alla specifica finalità del trattamento. Ne consegue che i dati non più necessari e quelli non utili devono essere smaltiti, in base alle seguenti procedure:

- MISURE ORGANIZZATIVE: Definizione di istruzioni chiare per il personale, riguardanti l'eliminazione del dato, come ad esempio la revisione periodica delle cartelle, la selezione dei documenti "scaduti", ovvero che hanno superato il termine legale di conservazione e la conseguente eliminazione del dato elettronico con lo spostamento dello stesso nel "cestino", e svuotamento di quest'ultimo (ove non automatico).
- MISURE TECNICHE: cancellazione del dato in modo definitivo dal database; formattazione del computer al momento di cambio di utente (in caso di nuova assunzione).

8.3 SISTEMA DI GESTIONE

La conformità legislativa e l'attuazione di misure di sicurezza tecniche ed organizzative adeguate rappresenta solo il primo passo per realizzare la protezione dei dati personali in termini sostanziali.

Il GDPR, che abbiamo visto essere una norma rivoluzionaria, pone delle sfide importanti in capo agli operatori del mercato. I principi di *privacy by design* e *privacy by default* su cui si costruisce il Regolamento lasciano intendere che gli obblighi di tutela non possono essere assolti unicamente attraverso un processo

di conformità al sistema normativo. Infatti, secondo il legislatore europeo, la protezione dei dati personali deve costituire il modo di pensare e di operare di un'organizzazione.

Ciò si traduce nella necessità di dotarsi di dinamiche di *management* interne che consentano di mantenere, nel tempo, quanto predisposto a protezione dei dati personali.

Il sistema di gestione rappresenta lo strumento per assicurare tale risultato. Implementare una struttura organizzativa (*ergo*, sistema di gestione) significa far sì che la gestione *privacy* entri a far parte dei processi aziendali, e che le attività ad essa connesse vengano svolte in modo naturale, fisiologico.

IN PRATICA

Cerchiamo di fare un esempio. Nel corso della normale attività quotidiana della Scuola di sci può succedere che, stagionalmente, il personale amministrativo impiegato venga sostituito. Il GDPR prevede che ogni soggetto che abbia accesso ai dati trattati dal Titolare del trattamento debba essere istruito da quest'ultimo. Le istruzioni vengono formalizzate nell'atto di nomina ad "Autorizzato al trattamento".

Dopo una prima designazione del dipendente amministrativo, c'è garanzia che l'arrivo di un nuovo collaboratore comporti in modo automatico la nuova nomina?

Attraverso un modello di gestione possono essere definite delle procedure integrate al processo di gestione del personale, che diano esito di quali siano le azioni da effettuare in ambito privacy (cfr. pag. 45).

La tutela, in questo senso, assumerà una dimensione di continuità.

In aggiunta, questo meccanismo consentirà anche di verificare l'efficacia e l'efficienza delle operazioni poste a protezione dei dati personali, attraverso meccanismi di audit/controllo interni ed esterni, e l'eventuale aggiornamento, laddove le medesime si rivelino obsolete o inidonee a realizzare il risultato perseguito.

Ulteriormente, nell'ambito di questo aspetto, vengono cristallizzati i processi e le azioni da intraprendere per valutare e gestire rischi inerenti ai singoli processi aziendali, in riferimento al contesto (economico, sociale, territoriale…) in cui opera la Scuola di sci;

In sintesi, la finalità del sistema di gestione è quella di garantire la conformità normativa e di stabilire procedure da seguire per proteggere i dati personali.

In seguito, si propone un esempio di sistema di gestione *privacy* a matrice, che considera, nello specifico, la procedura di gestione del personale, individuando gli adempimenti da compiere, ed il soggetto incaricato di eseguirli (E = esecutore; R = referente).

MATRICE DELLE PROCEDURE

SISTEMA DI GESTIONE PER LA PROTEZIONE DEI DAT PERSONALI

REV.00
D.E. 25.05.2018

RIFERIMENTO PROCEDURA N°	REV	ATTIVITA' DI DETTAGLIO	MODALITA' OPERATIVE (COME)	RESPONSABILITA' (CHI)				DOCUMENTI DI ORIGINE ESTERNA	REGISTRAZIONI
				DIRETTORE/ PRESIDENTE	AMMINISTRAZIONE	ADDETTO SEGRETERIA/VFRONT OFFICE	MAESTRI DI SCI		
				DIR	A	AS	MS		
PG. 01		GESTIONE CLIENTI							
PG. 02		GESTIONE FORNITORI							
PG. 03		GESTIONE PERSONALE							
PG.03	00	GESTIONE CV	Il CV può essere inviato tramite la sezione "Lavora con noi sul sito internet", nonchè tramite posta elettronica all'indirizzo info@scuoladisci.it, oppure consegnato in forma cartaceo presso la sede della Scuola di sci. I CV ricevuti in formato cartaceo vengono scannerizzati e salvati assieme a quelli raccolti in formato digitale all'interno del server aziendale nella cartella "CV nuove risorse". I CV vengono conservati sul server azienzale per 10 anni.	R		E		CV	
			L'informativa relativa al trattamento dei dati presenti nel CV viene pubblicata sul sito internet nella sezione "Lavora con noi", inviata via mail qualora il CV vengano raccolti via mail e consegnata in formato cartaceo se il CV viene depositato fisicamente presso la sede della Scuola di sci.	R				Nessuna documentazione	INFORMATIVA - GESTIONE CV
PG.03	00	ASSUNZIONE	All'atto dell'assunzione il DATORE DI LAVORO consegna al neo assunto il contratto di lavoro con allegata l'informativa concernente il trattamento dei dati e il relativo modulo di consenso. Contratto di lavoro, informativa e modulo di consenso, una volta sottoscritti vengono consegnati all'amministrazione perchè provveda al salvataggio nel server aziendale, all'interno della cartella "Personale".	R		E		Nessuna documentazione	CLAUSOLA CONTRATTUALE - DI RINVIO INFORMATIVA CONSENSO
			In base alla mansione viene predisposta la nomina ad "Autorizzato al tratamento" specifica per il singolo assunto, con indicazione dei trattamenti autorizzati e le istruzioni concernenti le modalità con cui deve essere effettuato il trattamento. Una copia della nomina verrà rilasciata al neo assunto e una salvata nel server aziendale.					Nessuna documentazione	NOMINA AD AUTORIZZATO AL TRATTAMENTO
PG.03	00	MANCATA ASSUNZIONE							
PG.03		CAMBIO MANSIONE							
PG.03	00	SORVEGLIANZA SANITARIA							
PG.03	00	INFORTUNIO							

L'approccio metodologico appena descritto è mutuato dalla normazione tecnica – o standard volontari – ed in particolare dalle linee guida ISO 9001:2015 e ISO/IEC 27001. Questo perché, ad oggi, non esiste ancora una norma tecnica specifica in materia di protezione dei dati.

La standard ISO 9001:2015 richiede alle aziende di condurre un'analisi del proprio contesto operativo e, contestualmente, procedere alla disamina dei rischi inficianti la qualità del proprio processo per l'erogazione del servizio o prodotto, in ottica di soddisfazione del cliente.

La norma ISO/IEC 27001, invece, declina il metodo menzionato delineando uno standard per la sicurezza delle informazioni e dei dati, principalmente a livello informatico.

È evidente la similarità della metodologia descritta con la disciplina dettata dal GDPR, in quanto anch'esso prescrive un'amministrazione dei dati personali affrontata in termini di rischio.

L'art. 24 GDPR stabilisce, infatti, che il Titolare del trattamento *tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*.

Cercando di semplificare, l'attività posta alla base della costruzione di un sistema di gestione, secondo i principi definiti dalle norme tecniche citate, può essere sintetizzata in alcuni passaggi cardine.

1.PLAN/PIANIFICAZIONE: analizzare i processi operativi che hanno ad oggetto il trattamento dei dati personali, e stabilire un obiettivo in termini di risultato per realizzare un adeguato livello di protezione dei dati personali, definendo contestualmente gli strumenti da utilizzare per il raggiungimento dello stesso.

2. DO/FARE: attuazione di quanto pianificato, attraverso l'adozione di misure tecniche ed organizzative (es. definizione di istruzioni chiare per il personale, applicazione misure tecniche informatiche, etc.)

3. CHECK/VERIFICARE: monitoraggio e misurazione dei risultati attraverso controlli effettuati da personale interno e risorse esterne (enti di certificazione), al fine di individuare eventuali scostamenti dagli obbiettivi prefissati, nonché cause e rimedi connessi.

4. ACT/AGIRE: attuazione delle soluzioni individuate per eliminare il discostamento dagli obbiettivi fissati in fase di pianificazione.

Inoltre, per una corretta applicazione del sistema di gestione, è necessario impiegare nella maniera più performante e soddisfacente le risorse umane, individuando per ogni risorsa un profilo, e quindi la posizione e le Responsabilità affidate relativamente al trattamento dei dati. Per raggiungere questo obiettivo, si procede con la costruzione dell'organigramma e l'individuazione dei compiti assegnati alle varie figure.

Ancora, il sistema di gestione implica la produzione di documenti a completamento dello stesso, i quali permettono di attuare correttamente il principio di *accountability* (che significa appunto, documentare il proprio operato).

Si tenga conto che l'Autorità Garante per la protezione dei dati personali ha avuto modo di affermare, a più riprese, che la presenza di un sistema di gestione, anche non certificato, costituisce prova della sussistenza di misure di sicurezza adeguate (provvedimento n. 513, 12 novembre 2014; provvedimento n. 68, 13 febbraio 2014).

L'adozione di un sistema di gestione, unitamente ad un modello organizzativo gestionale, potrebbe inoltre valere quale esimente della responsabilità amministrativa dell'ente per i reati presupposto elencati all'art. 24 *bis* del d.lgs. 231/2001, che riguarda i "delitti informatici e trattamento illecito di dati".

STRUMENTI OPERATIVI

9 STRUMENTI OPERATIVI

È importante ricordare che, quando l'Associato utilizza i dati personali, deve operare secondo le modalità di utilizzo richieste da AMSI Nazionale nel presente documento, volto ad identificare gli ambiti di operatività interessati dalla normativa sulla protezione dei dati personali, con conseguente definizione del *modus operandi*. Pertanto, è fondamentale dotarsi degli strumenti operativi suggeriti in questo paragrafo. Tuttavia, si ricorda che i modelli hanno carattere generale ed è necessaria un'azione di adeguamento specifica, non solo con riferimento alle parti evidenziate, ma in relazione ad ogni singolo aspetto (si pensi all'informativa per i clienti: se non si effettuano video o fotografie non sarà necessario specificare il trattamento relativo alla diffusione, e quindi non servirà nemmeno la liberatoria per l'utilizzo delle immagini). Gli strumenti disponibili sono i seguenti:

- INFORMATIVA DESTINATA AI CLIENTI;
- INFORMATIVA DESTINATA AI DIPENDENTI, AI MAESTRI ASSOCIATI, AI COLLABORATORI;
- INFORMATIVA DESTINATA AI COLLABORATORI;
- NOMINA AD AUTORIZZATO AL TRATTAMENTO DATI E ISTRUZIONI OPERATIVE: questo documento è destinato solo allo specifico dipendente, maestro assunto, associato, o collaboratore che, all'interno dell'associazione, esegue trattamenti su dati personali;
- NOMINA A RESPONSABILE DEL TRATTAMENTO: è rivolta ai soggetti esterni che trattano dati per conto del Titolare;
- REGISTRO DEI TRATTAMENTI: questo registro sarà più o meno corposo in base alla realtà considerata. La sua finalità è quella di dare conto, in maniera sistematica, di tutte le attività svolte dalla Scuola di Sci associata. Ad esempio, il trattamento considerato nel modello, che interessa l'area amministrativa, riguarda l'iscrizione del cliente alle lezioni di sci. A questa attività andranno aggiunti ulteriori trattamenti effettuati dall'area, come la gestione dei pagamenti, la programmazione delle gare di fine stagione, o ancora l'organizzazione dell'archivio cartaceo. Ulteriori aree da analizzare saranno, poi, la direzione, la segreteria, e l'insegnamento della pratica sportiva;
- REGISTRO DELLE VIOLAZIONI: tale strumento coadiuva il Titolare nel documentare qualsiasi violazione di dati che può intervenire nell'attività. Questo favorisce, ad esempio, una celere notificazione della violazione all'Autorità di controllo competente, nonché all'Interessato.

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 13 DEL REGOLAMENTO UE 2016/679 E DELL'ART. 13 D.LGS. 196/2003.

Premessa

Gentile Cliente, il "Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati", prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

(inserire dati dell'Associato: Scuola XY, oppure Maestro XY se lavora in autonomia), in qualità di "Titolare" del trattamento, ai sensi dell'articolo 13 del Reg. UE 2016/679, desidera illustrarLe le finalità e le modalità con cui vengono raccolti e trattati I Suoi dati personali.

In particolare, Le forniamo le seguenti informazioni:

1. Identità e dati di contatto del titolare:

Titolare del trattamento dei dati è **(inserire dati dell'Associato: Scuola XY, oppure Maestro XY se lavora in autonomia)** –P.IVA _____ –, con sede legale in _____.
Sarà possibile contattare il titolare del trattamento usando i seguenti recapiti:

- Tel: _____
- Mail: _____
- Pec:_____

2. Finalità del trattamento e base giuridica (selezionare solo le finalità che si riferiscono al singolo caso):

La raccolta ovvero il trattamento dei dati personali avviene per il perseguimento delle seguenti finalità:

- Finalità di contatto inerenti all'esecuzione e alla gestione del contratto;
- Adempimenti connessi all'instaurazione ed alla gestione del rapporto contrattuale;
- Gestione dell'eventuale contenzioso;
- Finalità di marketing diretto e invio di newsletter;
- Diffusione (con le modalità indicate alla lett. c) del presente articolo).

a) Adempimento di obblighi di legge a cui è soggetto il Titolare del trattamento (art. 6 co. 1 l. c) GDPR) ed esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (art. 6 co. 1 l. b) GDPR)

I Suoi dati personali saranno trattati esclusivamente per le finalità connesse all'adempimento delle obbligazioni contrattuali relative all'assistenza, all'insegnamento ed al supporto nell'attività sciistica.

b) Trattamento di particolari categorie di dati (art. 9 co. 2 lett. a) GDPR)

Il trattamento di particolari categorie di dati (come ad esempio dati relativi all' infortunio, o informazioni relative ad allergie ed intolleranze alimentari etc.) è subordinato al consenso espresso e specifico proveniente dall'Interessato, fornito in calce alla presente informativa.
Il conferimento di tali dati è obbligatorio. Pertanto, il mancato conferimento dei dati comporterà la possibilità da parte del Titolare di procedere alla costituzione del rapporto di lavoro.

c) Consenso alla diffusione (art. 9 co. 2 lett. a) GDPR)

Ulteriormente, previo Suo preventivo esplicito e facoltativo consenso prestato in calce alla presente informativa, nell'ambito della fruizione del servizio il Titolare potrà raccogliere e pubblicare fotografie e video ritraenti l'Interessato e/o il Minore, in occasione delle lezioni e in generale in occasione delle attività all'aperto, per finalità informative e di promozione circa le attività svolte dal Titolare del Trattamento.

La diffusione di tali contenuti (foto/video) avverrà su siti web, canali social e/o social network, a titolo esemplificativo e non esaustivo, Twitter, Instagram, YouTube, Pinterest, LinkedIn. Si informa, inoltre, che il consenso alla raccolta e alla diffusione di tali contenuti è completamente gratuito, e pertanto i sottoscritti si impegnano a rinunciare a qualsiasi voglia corrispettivo possa derivare dall'utilizzo dei contributi.
Il consenso al trattamento di immagini foto/video per le finalità promozionali sopra indicate è facoltativo e l'eventuale Suo rifiuto non avrà conseguenze circa la possibilità di usufruire della struttura e dei servizi forniti dal Titolare (Scuola XY, Maestro XY).

3. Modalità del trattamento

In relazione alle indicate finalità, il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità stesse e comunque in modo da garantire la sicurezza e la riservatezza dei dati stessi nel rispetto della normativa citata in epigrafe.
È esclusa l'esistenza di processi decisionali automatizzati, compresa la cd. profilazione.

4. Categorie di soggetti terzi a cui i dati possono essere comunicati.

Il Titolare del Trattamento potrà comunicare i suoi dati personali alle seguenti categorie di soggetti:
- istituti assicurativi e legali;
- studi e società nell'ambito dei rapporti di assistenza e consulenza professionale;
- tecnici per manutenzione e gestione del computer.

Tali soggetti tratteranno i dati in qualità di Responsabili del trattamento per conto del Titolare.
Potrà richiedere l'elenco dei Responsabili del trattamento, utilizzando i dati di contatto del Titolare indicati al punto 1.
I dati non saranno diffusi, salvo Suo esplicito e facoltativo consenso alla diffusione di immagini su sito web/social media, come indicato nel punto 2, lett. c) della presente informativa.

5. Durata del trattamento e periodo di conservazione.

I Suoi dati saranno trattati per le finalità sopra indicate e più precisamente per le attività di amministrazione e gestione dell'eventuale contenzioso, per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("principio di limitazione della conservazione", art.5, Reg. UE 2016/679) o in base alle scadenze previste dalle norme di legge. La verifica sulla obsolescenza dei dati conservati in relazione alle finalità per cui sono stati raccolti viene effettuata periodicamente.

6. Trasferimento dei dati fuori dall'Unione Europea

I dati raccolti non saranno oggetto di trasferimento verso Paesi extra-europei *oppure* Il Titolare trasferirà i dati presso un paese terzo o ad un'organizzazione internazionale per il quale esiste/non esiste una decisione di adeguatezza della Commissione o, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili (nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma GDPR).

7. Diritti dell'interessato

Nella Sua qualità di interessato potrà far valere i diritti di cui agli artt. 15 e seguenti del Reg. UE 2016/679 di seguito riportati:
Diritti di accesso, rettifica, integrazione e cancellazione dei dati, portabilità, limitazione del trattamento e revoca del consenso prestato.

a) A norma del Reg. (UE) 2016/679 Lei ha diritto di richiedere al Titolare l'accesso ai Suoi dati, nonché la rettifica, l'integrazione o la cancellazione degli stessi. Entro 30 giorni dall'inoltro della richiesta, Le verrà fornito riscontro in forma scritta anche attraverso mezzi elettronici.
b) Ha inoltre diritto di opporsi al trattamento o di richiedere la limitazione dello stesso, per motivi legittimi e nelle ipotesi previste agli artt. 18 e 21, Reg. UE 2016/679.

c) Potrà revocare in qualsiasi momento il consenso al trattamento dei dati prestato per le finalità determinate nella presente informativa.
d) In ultimo potrà esercitare il diritto alla portabilità dei dati, richiedendo al Titolare la trasmissione degli stessi verso un altro titolare.

Per esercitare i diritti sopra indicati sarà sufficiente utilizzare uno dei dati di recapito del Titolare del trattamento indicati al punto 1.

Diritto di proporre reclamo all'Autorità di Controllo.

a) Ha il diritto di rivolgersi all'Autorità di controllo proponendo reclamo, laddove ritenga di i Suoi dati siano trattai in modo illegittimo e contrariamente alle prescrizioni legislative in materia.

_____, lì___/___/_____ _____

Luogo e data Firma leggibile per presa visione

Letta l'informativa relativa alle finalità di diffusione di immagini, di cui al punto 2 lett. c), dichiaro di acconsentire alla raccolta ed alla pubblicazione, da parte del Titolare, di fotografie e video ritraenti il/i responsabile/i e/o il/i Minore/i, in occasione delle lezioni e in generale in occasione delle attività all'aperto, sul sito web e/o canali social.
Il consenso al trattamento dei dati raccolti per le finalità promozionali sopra indicate è facoltativo e l'eventuale Suo rifiuto non avrà conseguenze circa la possibilità di usufruire della struttura e dei servizi forniti dal Titolare

□ Acconsento □ NON acconsento

Luogo, data _____ Firma _____

Firma _____

(in caso di Minore/i firma degli esercenti la potestà genitoriale)

(In caso di contratto in essere) SCRITTURA INTEGRATIVA AL CONTRATTO (inserire riferimento al contratto)

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 13 DEL REGOLAMENTO UE 2016/679 E DELL'ART. 13 D.LGS. 196/2003.

Premessa

Gentile Interessato (*specificare se dipendente o collaboratore*), il "Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati", prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

(inserire dati dell'Associato: Scuola XY, oppure Maestro XY se lavora in autonomia), in qualità di "Titolare" del trattamento, ai sensi dell'articolo 13 del Reg. UE 2016/679, desidera illustrarLe le finalità e le modalità con cui vengono raccolti e trattati I Suoi dati personali.

In particolare, Le forniamo le seguenti informazioni:

1. Identità e dati di contatto del titolare:

Titolare del trattamento dei dati è **(inserire dati dell'Associato: Scuola XY, oppure Maestro XY se lavora in autonomia)** –P.IVA _____ –, con sede legale in _____.
Sarà possibile contattare il titolare del trattamento usando i seguenti recapiti:

- Tel: _____
- Mail: _____
- Pec: _____

8. Finalità del trattamento e base giuridica (selezionare solo le finalità che si riferiscono al singolo caso):

La raccolta ovvero il trattamento dei dati personali avviene per il perseguimento delle seguenti finalità:

- Finalità di contatto inerenti all'esecuzione e alla gestione del contratto;
- Adempimenti connessi all'instaurazione, gestione ed estinzione del rapporto di lavoro;
- Elaborazione e corresponsione delle retribuzioni;
- Assolvimento degli obblighi previdenziali, assistenziali, assicurativi, anche integrativi;
- Espletamento delle pratiche previste dalla normativa vigente in materia di sicurezza sul lavoro e protezione dei dati personali;
- Gestione dell'eventuale contenzioso;
- Diffusione (con le modalità indicate alla lett. c) del presente articolo).

d) Adempimento di obblighi di legge a cui è soggetto il Titolare del trattamento (art. 6 co. 1 l. c) GDPR) ed esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (art. 6 co. 1 l. b) GDPR)

I Suoi dati personali saranno trattati esclusivamente per le finalità connesse all'instaurazione, gestione ed estinzione del rapporto di lavoro. Più precisamente il trattamento dei dati personali, nonché di particolari categorie di dati, è finalizzato all'assolvimento degli obblighi di legge nascenti dal contratto di lavoro sottoscritto con il lavoratore e all'esercizio di diritti specifici dell'Interessato in materia di diritto del lavoro, previsti da norme comunitarie, leggi nazionali, ovvero da ulteriori fonti normative.

e) Consenso per il trattamento di particolari categorie di dati (art. 9 co. 2 lett. a) GDPR)

Il trattamento di particolari categorie di dati (come ad esempio l'appartenenza sindacale, dati sanitari desumibili da certificati attestanti assenze per maternità, infortunio, etc.) è subordinato al consenso espresso e specifico proveniente dall'Interessato, fornito in calce alla presente informativa.
Il conferimento di tali dati è obbligatorio. Pertanto, il mancato conferimento dei dati comporterà la possibilità da parte del Titolare di procedere alla costituzione del rapporto di lavoro.

f) Consenso alla diffusione (art. 9 co. 2 lett. a) GDPR)
Ulteriormente, previo Suo preventivo esplicito e facoltativo consenso prestato in calce alla presente informativa, nell'ambito della fruizione del servizio il Titolare potrà raccogliere e pubblicare fotografie e video ritraenti l'Interessato, in occasione delle lezioni e in generale in occasione delle attività all'aperto, per finalità informative e di promozione circa le attività svolte dal Titolare del Trattamento.
La diffusione di tali contenuti (foto/video) avverrà su siti web, canali social e/o social network, a titolo esemplificativo e non esaustivo, Twitter, Instagram, YouTube, Pinterest, LinkedIn. Si informa, inoltre, che il consenso alla raccolta e alla diffusione di tali contenuti è completamente gratuito, e pertanto i sottoscritti si impegnano a rinunciare a qualsiasi voglia corrispettivo possa derivare dall'utilizzo dei contributi.
Il consenso al trattamento di immagini foto/video per le finalità promozionali sopra indicate è facoltativo e l'eventuale Suo rifiuto non avrà conseguenze circa l'esecuzione del contratto stipulato con il Titolare (Scuola XY, Maestro XY).

9. Modalità del trattamento
In relazione alle indicate finalità, il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità stesse e comunque in modo da garantire la sicurezza e la riservatezza dei dati stessi nel rispetto della normativa citata in epigrafe.
È esclusa l'esistenza di processi decisionali automatizzati, compresa la cd. profilazione.

10. Categorie di soggetti terzi a cui i dati possono essere comunicati.
Il Titolare del Trattamento potrà comunicare i suoi dati personali alle seguenti categorie di soggetti:
- enti pubblici istituzionalmente investiti di funzioni legate al rapporto di lavoro (INPS, INAIL, DIREZIONE PROVINCIALE DEL LAVORO, etc.);
- soggetti giuridici istituzionalmente deputati all'assistenza integrativa, complementare e sanitaria su base negoziale;
- studi e società nell'ambito dei rapporti di assistenza e consulenza professionale;
- istituti di credito o banche per il pagamento delle competenze dovute;
- istituti assicurativi e legali;
- tecnici per manutenzione e gestione del computer.

Tali soggetti tratteranno i dati in qualità di Responsabili del trattamento per conto del Titolare.
Potrà richiedere l'elenco dei Responsabili del trattamento, utilizzando i dati di contatto del Titolare indicati al punto 1.
I dati non saranno diffusi, salvo Suo esplicito e facoltativo consenso alla diffusione di immagini su sito web/social media, come indicato nel punto 2, lett. c) della presente informativa.

11. Durata del trattamento e periodo di conservazione.
I Suoi dati saranno trattati per le finalità sopra indicate e più precisamente per le attività di amministrazione, contabilità, gestione paghe, formazione del personale, contrattuali e giuslavoristiche, gestione dell'eventuale contenzioso, per un tempo di conservazione pari nel massimo a 10 anni, come stabilito per Legge dal disposto di cui all'art. 2220 C.C, e comunque per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("principio di limitazione della conservazione", art.5, Reg. UE 2016/679) o in base alle scadenze previste dalle norme di legge. La verifica sulla obsolescenza dei dati conservati in relazione alle finalità per cui sono stati raccolti viene effettuata periodicamente.

12. Trasferimento dei dati fuori dall'Unione Europea

I dati raccolti non saranno oggetto di trasferimento verso Paesi extra-europei *oppure* Il Titolare trasferirà i dati presso un paese terzo o ad un'organizzazione internazionale per il quale esiste/non esiste una decisione di adeguatezza della Commissione o, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili (nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma GDPR).

13. Diritti dell'interessato

Nella Sua qualità di interessato potrà far valere i diritti di cui agli artt. 15 e seguenti del Reg. UE 2016/679 di seguito riportati:

Diritti di accesso, rettifica, integrazione e cancellazione dei dati, portabilità, limitazione del trattamento e revoca del consenso prestato.

e) A norma del Reg. (UE) 2016/679 Lei ha diritto di richiedere al Titolare l'accesso ai Suoi dati, nonché la rettifica, l'integrazione o la cancellazione degli stessi. Entro 30 giorni dall'inoltro della richiesta, Le verrà fornito riscontro in forma scritta anche attraverso mezzi elettronici.
f) Ha inoltre diritto di opporsi al trattamento o di richiedere la limitazione dello stesso, per motivi legittimi e nelle ipotesi previste agli artt. 18 e 21, Reg. UE 2016/679.
g) Potrà revocare in qualsiasi momento il consenso al trattamento dei dati prestato per le finalità determinate nella presente informativa.
h) In ultimo potrà esercitare il diritto alla portabilità dei dati, richiedendo al Titolare la trasmissione degli stessi verso un altro titolare.

Per esercitare i diritti sopra indicati sarà sufficiente utilizzare uno dei dati di recapito del Titolare del trattamento indicati al punto 1.

Diritto di proporre reclamo all'Autorità di Controllo.

b) Ha il diritto di rivolgersi all'Autorità di controllo proponendo reclamo, laddove ritenga di i Suoi dati siano trattai in modo illegittimo e contrariamente alle prescrizioni legislative in materia.

_____, lì___/___/_____ _____

Luogo e data Firma leggibile per presa visione

Consenso al trattamento dei dati per le finalità di cui all'art. 2 lett. c) della presente informativa.

Letta l'informativa relativa alle finalità di diffusione di immagini, di cui al punto e lett. c), dichiaro di acconsentire alla raccolta ed alla pubblicazione, da parte del Titolare, di fotografie e video ritraenti l'Interessato, in occasione delle lezioni e in generale in occasione delle attività all'aperto, sul sito web e/o canali social.

Il consenso al trattamento dei dati raccolti per le finalità promozionali sopra indicate è facoltativo e l'eventuale Suo rifiuto non avrà conseguenze circa l'esecuzione del contratto stipulato con il Titolare.

□ Acconsento □ NON acconsento

Luogo, data _____ _____

Firma leggibile

(In caso di contratto in essere) SCRITTURA INTEGRATIVA AL CONTRATTO (inserire riferimento al contratto)

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 13 DEL REGOLAMENTO UE 2016/679 E DELL'ART. 13 D.LGS. 196/2003.

Premessa

Gentile Fornitore, il "Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati", prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

(inserire dati dell'Associato: Scuola XY, oppure Maestro XY se lavora in autonomia), in qualità di "Titolare" del trattamento, ai sensi dell'articolo 13 del Reg. UE 2016/679, desidera illustrarLe le finalità e le modalità con cui vengono raccolti e trattati I Suoi dati personali.

In particolare, Le forniamo le seguenti informazioni:

1. Identità e dati di contatto del titolare:

Titolare del trattamento dei dati è **(inserire dati dell'Associato: Scuola XY, oppure Maestro XY se lavora in autonomia)** –P.IVA _____ –, con sede legale in _____.
Sarà possibile contattare il titolare del trattamento usando i seguenti recapiti:

- Tel: _____
- Mail: _____
- Pec:_____

14. Finalità del trattamento e base giuridica (selezionare solo le finalità che si riferiscono al singolo caso):

La raccolta ovvero il trattamento dei dati personali avviene per il perseguimento delle seguenti finalità:

- Finalità di contatto inerenti all'esecuzione e alla gestione del contratto;
- Adempimenti connessi all'instaurazione, gestione ed estinzione del rapporto di lavoro;
- Assolvimento degli obblighi previdenziali, assistenziali, assicurativi, anche integrativi;
- Espletamento delle pratiche previste dalla normativa vigente in materia di sicurezza sul lavoro e protezione dei dati personali;
- Gestione dell'eventuale contenzioso;

g) Adempimento di obblighi di legge a cui è soggetto il Titolare del trattamento (art. 6 co. 1 l. c) GDPR) ed esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (art. 6 co. 1 l. b) GDPR)

I Suoi dati personali saranno trattati esclusivamente per le finalità connesse all'instaurazione, gestione ed estinzione del rapporto di lavoro. Più precisamente il trattamento dei dati personali, è finalizzato all'assolvimento degli obblighi di legge nascenti dal contratto di lavoro sottoscritto con il lavoratore e all'esercizio di diritti specifici dell'Interessato in materia di diritto del lavoro, previsti da norme comunitarie, leggi nazionali, ovvero da ulteriori fonti normative.

15. Modalità del trattamento

In relazione alle indicate finalità, il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità stesse e comunque in modo da garantire la sicurezza e la riservatezza dei dati stessi nel rispetto della normativa citata in epigrafe.
È esclusa l'esistenza di processi decisionali automatizzati, compresa la cd. profilazione.

16. Categorie di soggetti terzi a cui i dati possono essere comunicati.
Il Titolare del Trattamento potrà comunicare i suoi dati personali alle seguenti categorie di soggetti:
• enti pubblici istituzionalmente investiti di funzioni legate al rapporto di lavoro (INPS, INAIL, DIREZIONE PROVINCIALE DEL LAVORO, etc.);
• soggetti giuridici istituzionalmente deputati all'assistenza integrativa, complementare e sanitaria su base negoziale;
• studi e società nell'ambito dei rapporti di assistenza e consulenza professionale;
• istituti di credito o banche per il pagamento dei corrispettivi dovuti;
• istituti assicurativi e legali;
• tecnici per manutenzione e gestione del computer.
Tali soggetti tratteranno i dati in qualità di Responsabili del trattamento per conto del Titolare.
Potrà richiedere l'elenco dei Responsabili del trattamento, utilizzando i dati di contatto del Titolare indicati al punto 1.

17. Durata del trattamento e periodo di conservazione.
I Suoi dati saranno trattati per le finalità sopra indicate e più precisamente per le attività di amministrazione, contabilità, gestione paghe, formazione del personale, contrattuali e giuslavoristiche, gestione dell'eventuale contenzioso, per un tempo di conservazione pari nel massimo a 10 anni, come stabilito per Legge dal disposto di cui all'art. 2220 C.C e comunque per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("principio di limitazione della conservazione", art.5, Reg. UE 2016/679) o in base alle scadenze previste dalle norme di legge. La verifica sulla obsolescenza dei dati conservati in relazione alle finalità per cui sono stati raccolti viene effettuata periodicamente.

18. Trasferimento dei dati fuori dall'Unione Europea
I dati raccolti non saranno oggetto di trasferimento verso Paesi extra-europei *oppure* Il Titolare trasferirà i dati presso un paese terzo o ad un'organizzazione internazionale per il quale esiste/non esiste una decisione di adeguatezza della Commissione o, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili (nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma GDPR).

19. Diritti dell'interessato
Nella Sua qualità di interessato potrà far valere i diritti di cui agli artt. 15 e seguenti del Reg. UE 2016/679 di seguito riportati:
Diritti di accesso, rettifica, integrazione e cancellazione dei dati, portabilità, limitazione del trattamento e revoca del consenso prestato.

i) A norma del Reg. (UE) 2016/679 Lei ha diritto di richiedere al Titolare l'accesso ai Suoi dati, nonché la rettifica, l'integrazione o la cancellazione degli stessi. Entro 30 giorni dall'inoltro della richiesta, Le verrà fornito riscontro in forma scritta anche attraverso mezzi elettronici.
j) Ha inoltre diritto di opporsi al trattamento o di richiedere la limitazione dello stesso, per motivi legittimi e nelle ipotesi previste agli artt. 18 e 21, Reg. UE 2016/679.
k) Potrà revocare in qualsiasi momento il consenso al trattamento dei dati prestato per le finalità determinate nella presente informativa.
l) In ultimo potrà esercitare il diritto alla portabilità dei dati, richiedendo al Titolare la trasmissione degli stessi verso un altro titolare.

Per esercitare i diritti sopra indicati sarà sufficiente utilizzare uno dei dati di recapito del Titolare del trattamento indicati al punto 1.

Diritto di proporre reclamo all'Autorità di Controllo.

c) Ha il diritto di rivolgersi all'Autorità di controllo proponendo reclamo, laddove ritenga di i Suoi dati siano trattai in modo illegittimo e contrariamente alle prescrizioni legislative in materia.

_____, lì___/___/_____ _____

Luogo e data Firma leggibile per presa visione

Nomina ad autorizzato al trattamento e istruzioni operative
Ai sensi degli artt. 24, co. 1 e 29, co. 1 – Reg. (UE) 2016/679

(**SCUOLA XY o MAESTRO XY se lavora in autonomia**) in qualità di TITOLARE DEL TRATTAMENTO DATI
Premesso che

- Il Sig./la Sig.ra_____ (*dati del dipendente*) e **(SCUOLA XY o MAESTRO XY)** hanno stipulato in data ____.____.____, formale contratto per _____ (es. addetto all'amministrazione/segreteria/contabilità), la cui esecuzione comporta il trattamento di dati in titolarità della (**SCUOLA XY o MAESTRO XY)**;
- Ai sensi dell'art. 24, co. 1, il Titolare del trattamento, tenuto conto della natura dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato in conformità delle previsioni normative vigenti in materia;
- Il Reg. (UE) 2016/679 all'art 29, co 1 stabilisce che chiunque agisca sotto l'autorità del Responsabile o del Titolare del trattamento e che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento;

TUTTO CIÒ PREMESSO
DESIGNA

Il Sig./la Sig.ra_____ (*dati del dipendente*), AUTORIZZATO AL TRATTAMENTO DEI DATI in relazione all'espletamento dell'incarico formalmente assunto con la sottoscrizione del contratto indicato in premessa.

L'Autorizzato dovrà effettuare il trattamento dei dati solo nei limiti dell'incarico assunto ed in particolare in relazione alle specifiche finalità oggetto del contratto.

In dettaglio, l'autorizzato dovrà:

- (*se si rapporta direttamente con il cliente*), raccogliere solamente i dati strettamente necessari per l'espletamento dell'incarico, senza richiedere informazioni ulteriori, e provvedere tempestivamente a conservarli nel luogo indicato dal Titolare;
- adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal Titolare del trattamento;
- quando appositamente autorizzato all'accesso alle banche dati informatiche, custodire con attenzione le proprie credenziali di autenticazione ed ogni dispositivo che le contiene, ed evitare di operare su terminali altrui e/o di lasciare accessibile il sistema operativo in caso di allontanamento, anche temporaneo, dal posto di lavoro, al fine di evitare trattamenti non autorizzati;
- conservare i supporti informatici e/o cartacei contenenti i dati personali, in modo da evitare che siano accessibili a persone non autorizzate al trattamento dei dati medesimi o siano facilmente oggetto di danneggiamenti intenzionali o accidentali;
- con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
- copie di dati personali oggetto di trattamento devono essere effettuate esclusivamente se necessario e soltanto previa autorizzazione del Titolare del trattamento;

- in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Titolare del trattamento;
- segnalare al Titolare del trattamento eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza, al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- effettuare la comunicazione dei dati esclusivamente ai soggetti indicati dal Titolare del trattamento e secondo le modalità stabilite dai medesimi;
- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
- svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite, anche in futuro, dal Titolare del trattamento e, comunque, in modo lecito e secondo correttezza;
- fornire al Titolare del trattamento, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentirgli di svolgere efficacemente la propria attività di controllo;
- in generale, prestare la più ampia e completa collaborazione al Titolare del trattamento ed all'eventuale Responsabile del trattamento al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

L'Autorizzato al trattamento dei dati personali prende atto che opererà sotto la diretta autorità del Titolare del trattamento e che, alla cessazione del rapporto contrattuale in essere tra le parti, per qualsiasi causa intervenuta, cesserà immediatamente la legittimazione dell'Autorizzato, fatto salvo il tempo necessario a completare le operazioni di restituzione o cancellazione dei dati e della documentazione connessa al Titolare del trattamento.

Il contraente, apponendo la sottoscrizione al presente atto, ne accetta integralmente il contenuto, assumendo la qualifica di Autorizzato al trattamento dei dati personali ai sensi dell'art. 29, co 1 Reg. (UE) 2016/679.

Luogo_____, lì _____.

_____
Firma dell'Autorizzato

SCRITTURA PRIVATA INTEGRATIVI AL MANDATO:

ATTO FORMALE DI NOMINA A RESPONSABILE DEL TRATTAMENTO
in applicazione del "Regolamento europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" – Reg. (UE) 2016/679

(Dati Scuola XY o Maestro XY che lavora in autonomia) - C.F./P.IVA _____- con sede legale in _____;

- ***Titolare del trattamento*** -

(Dati del fornitore), – C.F./P.IVA _____ **–** con sede legale in _____ In persona del l.r._____;

- ***Responsabile del trattamento*** -

PREMESSO CHE:

- ai sensi dell'art. 28 del Reg. (UE) 2016/679 (di seguito indicato come GDPR) il Titolare del trattamento ha la facoltà di incaricare un soggetto terzo, individuato in una persona fisica, persona giuridica, una pubblica amministrazione ovvero qualsiasi altro ente, associazione od organismo, al trattamento dei dati in possesso dello stesso, per il raggiungimento delle finalità per cui sono stati raccolti;
- l'art. 28 del G.D.P.R. prevede che il Responsabile del trattamento sia individuato in quel soggetto che effettua un trattamento per conto del Titolare; il Responsabile del trattamento è dunque colui che gestisce le operazioni di trattamento di dati, rispondendo a precisi compiti operativi e di coordinamento, operando in posizione subordinata rispetto al Titolare del trattamento;
- il Titolare del trattamento, ai sensi dell'art. 28, par. 1, Reg. (UE) 2016/679, deve ricorrere a Responsabili del trattamento che prestino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di legge richiesti dalle disposizioni *pro tempore* vigenti in materia, e garantisca la tutela dei diritti dell'interessato (Il Responsabile dovrebbe allegare o indicare nel presente atto descrizione delle misure tecniche e organizzative che adotta);
- ai sensi dell'art. 28, co. 3, Reg. (UE) 2016/679, i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il Responsabile del trattamento al Titolare del Trattamento ed alle sue indicazioni circa la materia disciplinata e la durata del trattamento, nonché la natura e le finalità dello stesso, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.
- con la presente scrittura si intende espressamente revocare e sostituire ogni altro accordo insistente tra le parti inerente al trattamento dei dati personali.

Per effetto del presente atto ed in virtù del rapporto contrattuale in essere di cui al contratto _____, sottoscritto in data _____, **(Dati Scuola XY o Maestro XY che lavora in autonomia)** - C.F./P.IVA _____, con sede legale in _____, in qualità di Titolare del trattamento a cui competono le decisioni in ordine alle finalità e alle modalità del trattamento

NOMINA

(Dati del fornitore), – C.F./P.IVA _____ con sede legale in _____ in persona del l.r. _____, Responsabile del

trattamento dei dati personali connessi all'espletamento delle attività necessarie per l'esecuzione del Servizio oggetto del contratto summenzionato e per adempiere a tutti gli obblighi derivanti dallo stesso.

Il trattamento dei dati da parte del Responsabile del trattamento nell'espletamento del Servizio dovrà avvenire nel rispetto e nel limite delle istruzioni di seguito meglio specificate:

1. **Trattamenti affidati al Responsabile del trattamento**
   Il Titolare affida al responsabile del trattamento, il trattamento di dati personali relativamente ai seguenti compiti (indicare i trattamenti specifici che effettua il Responsabile sui dati del Titolare, ad esempio, elaborazione delle buste paghe in caso di commercialista; realizzazione di un video o un servizio fotografico in caso di videomaker o fotografo):
   a) _____
   b) _____

2. **Natura e finalità del trattamento**

I dati potranno essere trattati esclusivamente per dare esecuzione al rapporto professionale in essere tra le parti e per adempiere a tutti gli obblighi derivanti dello stesso. In alcun caso i dati potranno essere trattati per finalità diverse rispetto a quanto previsto dal rapporto di collaborazione intercorrente tra Titolare e Responsabile del trattamento.

3. **Tipo di dati personali e categorie di Interessati**

I dati personali che potranno essere trattati dal Responsabile del trattamento, sono quelli strettamente necessari all'espletamento delle prestazioni oggetto dei rapporti contrattuali summenzionati e riguarderanno unicamente i soggetti coinvolti nell'attività di trattamento previste.

4. **Durata del trattamento**

Il trattamento avrà durata pari alla durata del rapporto di collaborazione tra le parti.
All'esaurirsi del rapporto professionale, il Responsabile del trattamento non sarà più autorizzato ad eseguire i trattamenti per conto del Titolare del trattamento, né a conservare i dati personali connessi, salvo che diversa disposizione di legge ne preveda la conservazione.

5. **Doveri e compiti del Responsabile del trattamento**

Con la sottoscrizione della presente nomina il Responsabile del trattamento dovrà impegnarsi a garantire la correttezza del Trattamento, nonché la predisposizione di adeguate misure di sicurezza idonee ad assicurare un adeguato livello di protezione dei dati personali trattati per conto del Titolare. Nello specifico il responsabile dovrà:

a) eseguire soltanto i trattamenti funzionali alle mansioni ad esso attribuite dal Servizio e procedere al trattamento dei dati solo a fronte di precisa istruzione documentata da parte del Titolare del trattamento, anche con riferimento all'eventuale trasferimento di dati personali affidatigli verso Paese extra europei; laddove il trasferimento sia richiesto dal diritto dell'Unione Europea o dalla normativa nazionale cui è soggetto il Responsabile del trattamento, quest'ultimo dovrà informare il Titolare del trattamento circa l'esistenza di tale obbligo giuridico prima del trattamento.
   Qualora sorgesse la necessità di dar luogo a trattamenti sui dati del titolare del trattamento comunicati per l'espletamento del servizio oggetto del rapporto contrattuale in essere, diversi ed eccezionali rispetto a quelli di norma eseguiti, il Responsabile dovrà informare preventivamente il Titolare ed ottenerne l'autorizzazione;
b) garantire che le persone autorizzate al trattamento dei dati personali nell'ambito della propria struttura organizzativa, abbiano ricevuto adeguate istruzioni scritte concernenti le modalità del trattamento, in ottemperanza a quanto disposto dalla legge e dal presente atto di nomina. A titolo esemplificativo ma non esaustivo, il Responsabile del trattamento, nel designare per iscritto le

persone autorizzate al trattamento dovrà prescrivere che essi abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria all'adempimento dei compiti loro assegnati. Dovrà inoltre, verificare che questi ultimi applichino tutte le disposizioni in materia di sicurezza dei dati personali.
Sarà cura del Responsabile vincolare le personae autorizzate al trattamento, ad un adeguato obbligo legale di riservatezza e segretezza, anche per il periodo successivo all'estinzione del rapporto di collaborazione intrattenuto con il Responsabile, in relazione alle operazioni di trattamento da esse eseguite;

c) adottare tutte le misure di sicurezza previste dalla normativa ed in particolare, ove applicabili, le misure previste all'art.32 del GDPR;
d) assistere il Titolare del trattamento con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste degli Interessati avanzate nell'esercizio dei propri diritti. In occasione di eventuale ricevimento di siffatte istanze, il Responsabile del trattamento provvederà ad informare tempestivamente il Titolare del trattamento, inoltrando copia della richiesta pervenuta;
e) collaborare alle attività di revisione, vigilanza e controllo realizzate dal titolare del trattamento o da un altro soggetto da questi formalmente incaricato; a tal scopo il Responsabile riconosce al Titolare del trattamento e agli incaricati del medesimo, il diritto ad ottenere informazioni circa lo svolgimento delle operazioni di trattamento di cui al presente atto;
f) cancellare o restituire tutti i dati personali al termine del rapporto contrattuale cui riferisce la presente nomina, facendo salva la necessità di conservazione dei dati qualora espressamente richiesto dalla legge; in entrambi i casi il Responsabile del trattamento provvederà a rilasciare al Titolare del trattamento, dietro specifica richiesta, apposita dichiarazione scritta contenente l'attestazione dell'avvenuta distruzione o restituzione;
g) mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi fissati dal presente atto e dalla normativa di riferimento applicabile.
h) informare tempestivamente il titolare del trattamento qualora a Suo parere, un'istruzione ricevuta violi le disposizioni del GDPR o altre disposizioni nazionali o dell'Unione europea relative alla protezione dei dati personali;
i) comunicare senza indugio l'intervento di contestazioni da parte degli Interessati, nonché ispezioni o richieste provenienti dall'Autorità di controllo o dalle Autorità giudiziarie, ed ogni altra notizia rilevante in relazione al trattamento dei dati personali;
j) redigere, ai sensi dell'art. 30, p. 2 GDPR, qualora ne ricorrano i presupposti, il registro delle attività di trattamento.

6. **Intervento di Responsabili di secondo livello**

Con il presente atto, il Titolare del trattamento conferisce autorizzazione scritta generale e formale al Responsabile del trattamento a poter ricorrere a eventuali, ulteriori Responsabile del trattamento (Responsabili di secondo livello), nella prestazione del servizio.
Qualora il Responsabile del trattamento nominato, debba ricorrere per l'esecuzione della prestazione ad un ulteriore Responsabile di secondo livello, dovrà previamente informare per iscritto il Titolare del trattamento, che avrà diritto di opporsi entro **5 giorni lavorativi** dal ricevimento della comunicazione**.**
Il Responsabile del trattamento si impegna a selezionare gli eventuali Responsabili di secondo livello, tra soggetti che forniscano garanzie sufficienti circa la possibilità di mettere in atto misure tecniche e organizzative adeguate ad assicurare la tutela dei diritti e delle libertà degli Interessati dal trattamento assegnatigli;
Il trattamento dei dati da parte dei Responsabili di secondo livello intervenuti, dovrà realizzarsi nell'ambito di un rapporto contrattuale o altro atto giuridico idoneo, concluso con il Responsabile del Trattamento, che imponga i medesimi obblighi ed istruzioni previsti nel presente atto.

La procedura indicata al paragrafo 2 e 4 del presente articolo, dovrà trovare applicazione anche nel caso in cui Responsabile intenda revocare, sostituire o nominare ulteriori Responsabili di secondo livello.

7. **Limitazione di responsabilità**
In caso di inadempimento dei presenti obblighi o condotte difformi o contrarie rispetto alle legittime istruzioni da parte del Titolare (**Scuola XY o Maestro XY**), il Responsabile (**fornitore**) è considerato come titolare, e risponde per i danni cagionati a terzi dal trattamento dei dati ai sensi dell'art. 82 del GDPR, se non prova che l'evento dannoso non gli/le è in alcun modo imputabile.
Al fine di garantire il risarcimento effettivo nei confronti dell'interessato, se il Titolare ed il Responsabile sono coinvolti nel medesimo trattamento e sono responsabili del danno causato, essi rispondono solidalmente per l'intero ammontare del danno, fatto salvo il diritto di regresso.

8. **Obblighi e diritti del Titolare**
   a) Il Titolare del trattamento si impegna ad informare tempestivamente il responsabile fornendo istruzioni documentate in caso divariazioni o cambiamenti nelle operazioni di trattamento dei dati.
   b) In ragione dell'affidamento in *outsourcing* del trattamento, il Titolare dovrà vigilare sull'operato del Responsabile mediante esecuzione di audit o controlli specifici eseguibili ad opera del Titolare medesimo o attraverso la collaborazione di altro soggetto specificatamente incaricato. Nel caso in cui il Titolare del trattamento ravvisi elementi non conformi o condizioni in grado di minare la sicurezza dei dati affidati con potenziale pregiudizio per gli interessati, esorterà il Responsabile al fine di sanare le anomalie individuate, e nei casi di maggiore gravità, avrà facoltà di procedere alla revoca della presente nomina e alla chiusura del rapporto di collaborazione.

9. **Disposizioni finali**
Per quanto non espressamente previsto e non riportato nel presente atto formale di nomina, si rinvia alla normativa europea vigente in materia di protezione e sicurezza dei dati personali, nonché alla normativa nazionale prevista in materia.
La presente valga anche quale documento di "istruzione documentata" circa le modalità ed i limiti del trattamento dei dati personali affidati al Responsabile del trattamento nominato, passabile di integrazione in relazione a successive ed occorrende esigenze.

Letto, approvato e sottoscritto.

Luogo_____, lì_____

Il Titolare del trattamento

_____

Il Responsabile esterno per accettazione

_____

	A	B
1	Nome del Titolare del Trattamento	
2	**SCUOLA XY o MAESTRO XY che lavora in autonomia**	
3	SEDE	
4	DATI DI CONTATTO	Area amministrativa
5	Tel.	**Processo**
6	Fax	ISCRIZIONE ALLE LEZIONI DI SCI
7	Mail	
8	**Descrizione del Processo**	
9	Trattamento	Raccolta di dati del cliente che partecipa alle lezioni di sci. Le iscrizioni provengono anche da apposito form compilato dal cliente all'interno del sito web, via e - mail e da contatto telefonico dello stesso.
10	Modalità del trattamento	Consegna personale di modulo cartaceo, presso la sede, e registrazione delle informazioni sul gestionale interno; raccolta delle iscrizioni effettuate on - line (sul sito web o via e - mail) e telefonicamente ed
11	Diffusione	NO.
12	SW applicativi specifici (sistemi gestionali)	Gestionale XY - Mail XY - Sito web.
13	Categorie di interessati	CLIENTE (sia maggiorenne che minorenne).
14	Provenienza dei dati	Direttamente dall'interessato.
15		
16	**Liceità del trattamento**	
17	Base giuridica	Il trattamento è necessario per l'adempimento obblighi contrattuali e per interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati. Inoltre, è richiesto il consenso per la raccolta e la diffusione di
18	Consenso	Si.
19		
20	**Attori**	
21	Titolare del trattamento	SCUOLA XY o MAESTRO XY che lavora in autonomia
22	Responsabile della protezione dati - DPO	Non presente.
23	Autorizzati al trattamento (ufficio/area di riferimento)	Dati dei soggetti che si occupano della raccolta dei dati al momento dell'iscrizione alle lezioni, nonché del Maestro che effettua la lezione.
24	Contitolari del trattamento	NO
25	COMUNICAZIONE - Categoria di destinatari esterni (Responsabili del trattamento)	Specificare i responsabili che interessano lo specifico trattamento (ES: Assicurazione, servizio legale, fotografo, videomaker, tecnico informatico, tecnico o soggetto che gestisce il sito web e l'area social media).
26		
27	**Finalità del trattamento effettuato**	
28	Fianlità principale	Raccolta di dati del cliente per adempiere ad obbligazioni contrattuali relative allo svolgimento delle lezioni di sci.
29		
30	**Tipologia di dati personali interessati e descrizione**	
31	Dati comuni	Dati di identificazione personale, di contatto e bancari.
32	Dati particolari	Biometrici (foto e video idonee ad indentificare in modo univoco una persona); dati relativi all'infortunio, indicazioni relative ad intollranze alimentari.

34	**Conservazione**	
35	LUOGO CUSTODIA FILE (dati privilegi accesso ai sistemi)	Specificare il luogo elettronico di conservazione (es. server locale - server sito WEB).
36	LUOGO CUSTODIA CARTACEO	Specificare il luogo cartaceo di conservazione (es. armadietti ufficio amministrazione).
37	TEMPI CONSERVAZIONE / TERMINI ULTIMI PER LA CANCELLAZIONE	Norme di legge (10 anni).
38	Modalità di cancellazione /distruzione della documentazione cartacea	Specificare le modalità di cancellazione e distruzione (es. distruggi documenti).
39	Modalità di cancellazione dei dati informatici	Specificare le modalità di cancellazione e distruzione (es. spostamento del file nel cestino).
40		
41	**Trasferimenti al di fuori dell'UE**	NO
42		
43	**Misure di sicurezza**	
44	Misure di sicurezza tecniche ed organizzative generali	Specificare le misure di sicurezza generali (che valgono per ogni processo), come ad ES: Anti virus a protezione di tutti i client - Firewall - Backup gironaliero - Password di accesso ai client - strutturazione del server con diversi autorizzazioni di accesso - Chiusura ingresso principale dell'edificio - Allarme antintrusione.
45	Misure di sicurezza tecniche e organizzative specifiche del trattamento	Specificare le misure di sicurezza specifiche del singolo processo, come ad ES: Conservazione dei dati particolari, come le indicazioni relative ad infortunio del cliente, indicazioni relative ad intolleranze alimentari, immagini idonee ad identificare in modo univoco la persona, in armadietti chiusi a chiave, ignifughi.

SCUOLA XY o MAESTRO XY che lavora in autonomia		
SEDE		
DATI DI CONTATTO		
Tel.	**Registro delle violazioni (art. 33 GDPR)**	
Fax		
Mail		
	Il Titolare è tenuto a documentare qualsiasi violazione di dati ("violazione dei dati personali") che ai sensi dell'art. 4, punto 12, comporta, accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.	
Unità operativa preposta alla conservazione del registro	Indicare il soggetto che si occupa della redazione del registro	

TIPOLOGIA DI VIOLAZIONE DI DATI	DESCRIZIONE DELLA VIOLAZIONE	DATA	LUOGO	DATO	CONSEGUENZE	Provvedimenti adottati per porre rimedio alle violazioni
PUBBLICAZIONE NON AUTORIZZATA DI IMMAGINI SU "FACEBOOK" RITRAENTI UN SOGGETTO MINORE	Il Maestro XY ha pubblicato sulla propria pagina "Facebook" n. 2 immagini ritraenti un soggetto minore ed idonee ad identificarlo in modo non equivoco	31/12/...	Comprensorio sciistico Z	Fotografia	Perdita del controllo dei dati personali e conseguente diffusione (copia) dell'immagine su siti web anomali	Notificazione della violazione all'Autorità di controllo competente entro 72 ore; Comunicazione della violazione dei dati personali all'Interessato; Richiamo al Maestro XY; Rimozione dell'immagine; Esecuzione di una riunione informativa con tutti i Maestri volta alla sensibilizzazione sul tema
FURTO DI DOCUMENTI DEI CLIENTI CONTENENTI ANCHE DATI PARTICOLARI E DATI BANCARI	All'apertura della sede/ufficio il personale amministrativo ha constatato la forzatura della serratura, ed il futro di documentazione relativa ai pagamenti, archiviata negli scaffali situati nel locale d'ingresso, alle spalle del front office	02/03/...	Ufficio sito in ...	N. 3 fascicoli (A - M) contenente documenti	Perdita del controllo dei dati personali	Notificazione della violazione all'Autorità di controllo competente entro 72 ore; Denuncia del futro presso la Stazione CC di ...; Pubblicazione sul sito web di un avviso rivolto agli Interessati denunciante la violazione riscontrata; Spostamento dei fascicoli nella stanza interna, in armadio chiuso a chiave; Cambio della serratura e installazione di allarme antincendio.

REGISTRO DELLE VIOLAZIONI

QSA SRL - ENGINEERING CONSULTING TRAINING

C.F. - P.IVA.: 01670340221 - e-mail: info@qsa.it - pec: qsasrl@pec.it - tel: 0461 – 950720

WWW.QSA.IT